Algebra3, elemző szakirány

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
ewkiss@cs.elte.hu

3. előadás

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű:

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív,

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes,

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt.

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r prím: ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r prím: ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.
R alaptételes: minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r prím: ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.
R alaptételes: minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.
Főpéldák alaptételes gyűrűre:

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r prím: ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.
R alaptételes: minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.
Főpéldák alaptételes gyűrűre: $\mathbb{Z}$,

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r prím: ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.
R alaptételes: minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.
Főpéldák alaptételes gyűrűre: $\mathbb{Z}$, $T[x]$ (T test),

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r prím: ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.
R alaptételes: minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.
Főpéldák alaptételes gyűrűre: $\mathbb{Z}$, $T[x]$ (T test), $\mathbb{Z}[x]$.

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r prím: ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.
R alaptételes: minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.
Főpéldák alaptételes gyűrűre: $\mathbb{Z}$, $T[x]$ (T test), $\mathbb{Z}[x]$.
$a, b \in R$ kitüntetett közös osztója d, ha

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r prím: ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.
R alaptételes: minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.
Főpéldák alaptételes gyűrűre: $\mathbb{Z}$, $T[x]$ (T test), $\mathbb{Z}[x]$.
$a, b \in R$ kitüntetett közös osztója d, ha

(1) d közös osztó, azaz $d \mid a$ és $d \mid b$;

Számelméleti alapfogalmak

Ismétlés (3.1. Szakasz)

Szokásos gyűrű: kommutatív, nullosztómentes, egységelemes.
r osztója s-nek, ha van olyan t a gyűrűben, hogy $s = tr$.
Egység: mindent oszt. Legyen $r \in R$ nem nulla, nem egység.
Triviális felbontás: $r = ab$, ha valamelyik tényező egység.
r felbonthatatlan: nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).
r prím: ha $r \mid ab$, akkor $r \mid a$ vagy $r \mid b$.
R alaptételes: minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.
Főpéldák alaptételes gyűrűre: $\mathbb{Z}$, $T[x]$ (T test), $\mathbb{Z}[x]$.
$a, b \in R$ kitüntetett közös osztója d, ha

(1) d közös osztó, azaz $d \mid a$ és $d \mid b$;

(2) d mindegyik közös osztónak többszöröse.

Az alapfogalmak összefüggései

3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

Az alapfogalmak összefüggései

3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

3.1.28. Gyakorlat

Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel egyértelműségi állítása.

Az alapfogalmak összefüggései

3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

3.1.28. Gyakorlat

Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel egyértelműségi állítása.

3.1.22. és 3.1.26. Gyakorlatok

Alaptételes gyűrűben

Az alapfogalmak összefüggései

3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

3.1.28. Gyakorlat

Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel egyértelműségi állítása.

3.1.22. és 3.1.26. Gyakorlatok

Alaptételes gyűrűben

(1) bármely két elemnek van kitüntetett közös osztója;

Az alapfogalmak összefüggései

3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

3.1.28. Gyakorlat

Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel egyértelműségi állítása.

3.1.22. és 3.1.26. Gyakorlatok

Alaptételes gyűrűben

(1) bármely két elemnek van kitüntetett közös osztója;

(2) minden felbonthatatlan elem prím.

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll:

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

5.5.4. Lemma

$r \mid s \iff (r) \supseteq (s)$. □

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

5.5.4. Lemma

$r \mid s \iff (r) \supseteq (s)$. □

Figyelem: „Megfordul” a dolog!

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

5.5.4. Lemma

$r \mid s \iff (r) \supseteq (s)$. □

Figyelem: „Megfordul” a dolog!
Például 2 kisebb, mint 4,

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

5.5.4. Lemma

$r \mid s \iff (r) \supseteq (s)$. □

Figyelem: „Megfordul” a dolog!
Például 2 kisebb, mint 4, de (2) nagyobb, mint (4).

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

5.5.4. Lemma

$r \mid s \iff (r) \supseteq (s)$. □

Figyelem: „Megfordul” a dolog!
Például 2 kisebb, mint 4, de (2) nagyobb, mint (4).

Ismétlés (4.6.1. Állítás)

Legyen G Abel-csoport az összeadásra és $a, b \in G$.

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

5.5.4. Lemma

$r \mid s \iff (r) \supseteq (s)$. □

Figyelem: „Megfordul” a dolog!
Például 2 kisebb, mint 4, de (2) nagyobb, mint (4).

Ismétlés (4.6.1. Állítás)

Legyen G Abel-csoport az összeadásra és $a, b \in G$.
Ekkor az $na + mb$ alakú elemek H halmaza, ahol $n, m \in \mathbb{Z}$

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

5.5.4. Lemma

$r \mid s \iff (r) \supseteq (s)$. □

Figyelem: „Megfordul” a dolog!
Például 2 kisebb, mint 4, de (2) nagyobb, mint (4).

Ismétlés (4.6.1. Állítás)

Legyen G Abel-csoport az összeadásra és $a, b \in G$.
Ekkor az $na + mb$ alakú elemek H halmaza, ahol $n, m \in \mathbb{Z}$
a legszűkebb olyan részcsoport, amely a-t és b-t tartalmazza.

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

5.5.4. Lemma

$r \mid s \iff (r) \supseteq (s)$. □

Figyelem: „Megfordul” a dolog!
Például 2 kisebb, mint 4, de (2) nagyobb, mint (4).

Ismétlés (4.6.1. Állítás)

Legyen G Abel-csoport az összeadásra és $a, b \in G$.
Ekkor az $na + mb$ alakú elemek H halmaza, ahol $n, m \in \mathbb{Z}$
a legszűkebb olyan részcsoport, amely a-t és b-t tartalmazza.
Azaz ha $K \leq G$ és $a, b \in K$,

Ideálok és oszthatóság

Emlékeztető (5.1.10. Definíció)

(r) az r összes többszöröséből áll: főideál.

5.5.4. Lemma

$r \mid s \iff (r) \supseteq (s)$. □

Figyelem: „Megfordul” a dolog!
Például 2 kisebb, mint 4, de (2) nagyobb, mint (4).

Ismétlés (4.6.1. Állítás)

Legyen G Abel-csoport az összeadásra és $a, b \in G$.
Ekkor az $na + mb$ alakú elemek H halmaza, ahol $n, m \in \mathbb{Z}$
a legszűkebb olyan részcsoport, amely a-t és b-t tartalmazza.
Azaz ha $K \leq G$ és $a, b \in K$, akkor $H \subseteq K$.

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.
Azaz ha $K \triangleleft G$ és $a, b \in K$,

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.
Azaz ha $K \triangleleft G$ és $a, b \in K$, akkor $H \subseteq K$.

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.
Azaz ha $K \triangleleft G$ és $a, b \in K$, akkor $H \subseteq K$.

Bizonyítás: HF a 4.6.1. Állítás bizonyítása alapján.

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.
Azaz ha $K \triangleleft G$ és $a, b \in K$, akkor $H \subseteq K$.

Bizonyítás: HF a 4.6.1. Állítás bizonyítása alapján.

5.1.10. Definíció

Legyen R szokásos gyűrű és $a_1 \ldots, a_n \in R$.

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.
Azaz ha $K \triangleleft G$ és $a, b \in K$, akkor $H \subseteq K$.

Bizonyítás: HF a 4.6.1. Állítás bizonyítása alapján.

5.1.10. Definíció

Legyen R szokásos gyűrű és $a_1 \ldots, a_n \in R$.
Az $r_1 a_1 + \ldots + r_n a_n$ alakú elemek halmazát, ahol $r_1, \ldots, r_n \in R$,

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.
Azaz ha $K \triangleleft G$ és $a, b \in K$, akkor $H \subseteq K$.

Bizonyítás: HF a 4.6.1. Állítás bizonyítása alapján.

5.1.10. Definíció

Legyen R szokásos gyűrű és $a_1 \ldots, a_n \in R$.
Az $r_1 a_1 + \ldots + r_n a_n$ alakú elemek halmazát, ahol $r_1, \ldots, r_n \in R$,
az $a_1, \ldots, a_n$ által generált ideálnak nevezzük,

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.
Azaz ha $K \triangleleft G$ és $a, b \in K$, akkor $H \subseteq K$.

Bizonyítás: HF a 4.6.1. Állítás bizonyítása alapján.

5.1.10. Definíció

Legyen R szokásos gyűrű és $a_1 \ldots, a_n \in R$.
Az $r_1 a_1 + \ldots + r_n a_n$ alakú elemek halmazát, ahol $r_1, \ldots, r_n \in R$,
az $a_1, \ldots, a_n$ által generált ideálnak nevezzük, jele $(a_1, \ldots, a_n)$.

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.
Azaz ha $K \triangleleft G$ és $a, b \in K$, akkor $H \subseteq K$.

Bizonyítás: HF a 4.6.1. Állítás bizonyítása alapján.

5.1.10. Definíció

Legyen R szokásos gyűrű és $a_1 \ldots, a_n \in R$.
Az $r_1 a_1 + \ldots + r_n a_n$ alakú elemek halmazát, ahol $r_1, \ldots, r_n \in R$,
az $a_1, \ldots, a_n$ által generált ideálnak nevezzük, jele $(a_1, \ldots, a_n)$.

Ez a legszűkebb $a_1, \ldots, a_n$-et tartalmazó ideál,

Generált ideál

5.1.9. Állítás

Legyen R szokásos gyűrű és $a, b \in R$.
Ekkor az $ra + sb$ alakú elemek H halmaza, ahol $r, s \in R$
a legszűkebb olyan ideál, amely a-t és b-t tartalmazza.
Azaz ha $K \triangleleft G$ és $a, b \in K$, akkor $H \subseteq K$.

Bizonyítás: HF a 4.6.1. Állítás bizonyítása alapján.

5.1.10. Definíció

Legyen R szokásos gyűrű és $a_1 \ldots, a_n \in R$.
Az $r_1 a_1 + \ldots + r_n a_n$ alakú elemek halmazát, ahol $r_1, \ldots, r_n \in R$,
az $a_1, \ldots, a_n$ által generált ideálnak nevezzük, jele $(a_1, \ldots, a_n)$.

Ez a legszűkebb $a_1, \ldots, a_n$-et tartalmazó ideál,
a főideál általánosítása.

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$,

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$,

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$,

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

FIGYELEM! (a, b) nem mindig főideál!

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

FIGYELEM! (a, b) nem mindig főideál!

$R = \mathbb{Z}[x]$ alaptételes gyűrű,

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

FIGYELEM! (a, b) nem mindig főideál!

$R = \mathbb{Z}[x]$ alaptételes gyűrű, 2 és x kitüntetett közös osztója 1,

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

FIGYELEM! (a, b) nem mindig főideál!

$R = \mathbb{Z}[x]$ alaptételes gyűrű, 2 és x kitüntetett közös osztója 1, hiszen 2 osztói csak ± 1, ± 2,

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

FIGYELEM! (a, b) nem mindig főideál!

$R = \mathbb{Z}[x]$ alaptételes gyűrű, 2 és x kitüntetett közös osztója 1, hiszen 2 osztói csak ± 1, ± 2, és $2 \nmid x$.

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

FIGYELEM! (a, b) nem mindig főideál!

$R = \mathbb{Z}[x]$ alaptételes gyűrű, 2 és x kitüntetett közös osztója 1, hiszen 2 osztói csak ± 1, ± 2, és $2 \nmid x$.
$(2, x)$ azokból a polinomokból áll, melyek konstans tagja páros.

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

FIGYELEM! (a, b) nem mindig főideál!

$R = \mathbb{Z}[x]$ alaptételes gyűrű, 2 és x kitüntetett közös osztója 1, hiszen 2 osztói csak ± 1, ± 2, és $2 \nmid x$.
$(2, x)$ azokból a polinomokból áll, melyek konstans tagja páros.
Az 1 nem ilyen,

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

FIGYELEM! (a, b) nem mindig főideál!

$R = \mathbb{Z}[x]$ alaptételes gyűrű, 2 és x kitüntetett közös osztója 1, hiszen 2 osztói csak ± 1, ± 2, és $2 \nmid x$.
$(2, x)$ azokból a polinomokból áll, melyek konstans tagja páros.
Az 1 nem ilyen, tehát $(2, x) \neq (1)$,

Ideálok és kitüntetett közös osztó

5.5.5. Lemma

Legyen R szokásos gyűrű és $a, b \in R$.
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
(A kitüntetett közös osztót is (a, b) jelölte számelméletben.)

Bizonyítás

Mivel $(d) = (a, b) \supseteq (a)$, ezért $d \mid a$, ugyanígy $d \mid b$.
Ha $c \mid a$ és $c \mid b$, akkor $d = ra + sb$ miatt $c \mid d$. □

FIGYELEM! (a, b) nem mindig főideál!

$R = \mathbb{Z}[x]$ alaptételes gyűrű, 2 és x kitüntetett közös osztója 1, hiszen 2 osztói csak ± 1, ± 2, és $2 \nmid x$.
$(2, x)$ azokból a polinomokból áll, melyek konstans tagja páros.
Az 1 nem ilyen, tehát $(2, x) \neq (1)$, ezért $(2, x)$ nem főideál.

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,
és így nem is euklideszi,

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,
és így nem is euklideszi, noha alaptételes.)

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,
és így nem is euklideszi, noha alaptételes.)
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,
és így nem is euklideszi, noha alaptételes.)
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
Ezért főideálgyűrűben

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,
és így nem is euklideszi, noha alaptételes.)
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
Ezért főideálgyűrűben (és így euklideszi gyűrűben)

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,
és így nem is euklideszi, noha alaptételes.)
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
Ezért főideálgyűrűben (és így euklideszi gyűrűben)
bármely két elemnek van kitüntetett közös osztója.

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,
és így nem is euklideszi, noha alaptételes.)
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
Ezért főideálgyűrűben (és így euklideszi gyűrűben)
bármely két elemnek van kitüntetett közös osztója.
Így érvényes az alaptétel egyértelműségi állítása.

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,
és így nem is euklideszi, noha alaptételes.)
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
Ezért főideálgyűrűben (és így euklideszi gyűrűben)
bármely két elemnek van kitüntetett közös osztója.
Így érvényes az alaptétel egyértelműségi állítása.

Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

Euklideszi és főideálgyűrű alaptételes

Ismétlés

Euklideszi gyűrű: ahol elvégezhető a maradékos osztás.
Főideálgyűrű: ahol minden ideál főideál.
Beláttuk: minden euklideszi gyűrű főideálgyűrű.
(Az előző példa szerint $\mathbb{Z}[x]$ nem főideálgyűrű,
és így nem is euklideszi, noha alaptételes.)
Ha $(a, b) = (d)$, akkor d az a és b kitüntetett közös osztója.
Ezért főideálgyűrűben (és így euklideszi gyűrűben)
bármely két elemnek van kitüntetett közös osztója.
Így érvényes az alaptétel egyértelműségi állítása.

Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

A felbontás létezését nem bizonyítjuk.

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3$$

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is, $2 \pm i\sqrt{5}$ is felbonthatatlan,

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is, $2 \pm i\sqrt{5}$ is felbonthatatlan,
de 3 nem egységszerese $2 \pm i\sqrt{5}$-nek,

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is, $2 \pm i\sqrt{5}$ is felbonthatatlan,
de 3 nem egységszerese $2 \pm i\sqrt{5}$-nek,
így ez a 9-nek két, lényegesen különböző felbontása.

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is, $2 \pm i\sqrt{5}$ is felbonthatatlan,
de 3 nem egységszerese $2 \pm i\sqrt{5}$-nek,
így ez a 9-nek két, lényegesen különböző felbontása.
Ezért ez a gyűrű nem alaptételes.

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is, $2 \pm i\sqrt{5}$ is felbonthatatlan,
de 3 nem egységszerese $2 \pm i\sqrt{5}$-nek,
így ez a 9-nek két, lényegesen különböző felbontása.
Ezért ez a gyűrű nem alaptételes.

Az ilyen gyűrűk is hasznosak számelméleti problémák megoldásához.

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is, $2 \pm i\sqrt{5}$ is felbonthatatlan,
de 3 nem egységszerese $2 \pm i\sqrt{5}$-nek,
így ez a 9-nek két, lényegesen különböző felbontása.
Ezért ez a gyűrű nem alaptételes.

Az ilyen gyűrűk is hasznosak számelméleti problémák megoldásához. A kiút az, hogy a $(9, 3(2 + i\sqrt{5}))$ ideál veszi át a hiányzó kitüntetett közös osztó szerepét.

A kitüntetett közös osztó nemlétezése

Példa (3.1.34. Feladat)

Legyen R az $a + bi\sqrt{5}$ alakú számokból álló gyűrű ($a, b \in \mathbb{Z}$).
A 9-nek és a $3(2 + i\sqrt{5})$-nek nincs kitüntetett közös osztója.
A 3 felbonthatatlan, de nem prím.
Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is, $2 \pm i\sqrt{5}$ is felbonthatatlan,
de 3 nem egységszerese $2 \pm i\sqrt{5}$-nek,
így ez a 9-nek két, lényegesen különböző felbontása.
Ezért ez a gyűrű nem alaptételes.

Az ilyen gyűrűk is hasznosak számelméleti problémák megoldásához. A kiút az, hogy a $(9, 3(2 + i\sqrt{5}))$ ideál veszi át a hiányzó kitüntetett közös osztó szerepét.
Ez a témakör az algebrai számelmélet.