Algebra3, elemző szakirány

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
ewkiss@cs.elte.hu

9. előadás

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^+ additiv 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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s$

Karakterisztika: bizonyítás

Bizonyítás

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

Karakterisztika: bizonyítás

Bizonyítás

Tegyük föl, hogy $0 \neq r \in R$ és $0 \neq n \in \mathbb{Z}$, melyre $nr = 0$.
Az R^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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^+ additiv csoportban az elemrend jele $o(r)$.
Tehát n „jó kitevője” (együtthatója) r-nek, és így $m = o(r) \mid n$.
Persze $mr = 0$. Tetszőleges $s \in R$ esetén $0 = (mr)s = r(ms)$.
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 $P = \{(me)/(ne) \ : \ m, 0 \neq n \in \mathbb{Z}\}$ $\mathbb{Q}$-val izomorf résztest,

Prímtest 0 karakterisztikában

5.8.7. Tétel

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

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Bizonyítás

Legyen T karakterisztikája p, prímteste P,

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Bizonyítás

Legyen T karakterisztikája p, prímteste P, és $|T : P| = n$.

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Bizonyítás

Legyen T karakterisztikája p, prímteste P, és $|T : P| = n$.
Ekkor T elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban,

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Bizonyítás

Legyen T karakterisztikája p, prímteste P, és $|T : P| = n$.
Ekkor T elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis T-ben P fölött,

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Bizonyítás

Legyen T karakterisztikája p, prímteste P, és $|T : P| = n$.
Ekkor T elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis T-ben P fölött, és $\lambda_1, \ldots, \lambda_n \in P$.

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Bizonyítás

Legyen T karakterisztikája p, prímteste P, és $|T : P| = n$.
Ekkor T elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis T-ben P fölött, és $\lambda_1, \ldots, \lambda_n \in P$.
Mindegyik λ_i skalár $|P| = p$-féle lehet,

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Bizonyítás

Legyen T karakterisztikája p, prímteste P, és $|T : P| = n$.
Ekkor T elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis T-ben P fölött, és $\lambda_1, \ldots, \lambda_n \in P$.
Mindegyik λ_i skalár $|P| = p$-féle lehet, így $|T| = p^n$. □

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Bizonyítás

Legyen T karakterisztikája p, prímteste P, és $|T : P| = n$.
Ekkor T elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis T-ben P fölött, és $\lambda_1, \ldots, \lambda_n \in P$.
Mindegyik λ_i skalár $|P| = p$-féle lehet, így $|T| = p^n$. □

Megjegyzés

A $\lambda_1 b_1 + \ldots + \lambda_n b_n \mapsto (\lambda_1, \ldots, \lambda_n)$ megfeleltetés nyilván összegtartó.

Véges test elemszáma

6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

Bizonyítás

Legyen T karakterisztikája p, prímteste P, és $|T : P| = n$.
Ekkor T elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis T-ben P fölött, és $\lambda_1, \ldots, \lambda_n \in P$.
Mindegyik λ_i skalár $|P| = p$-féle lehet, így $|T| = p^n$. □

Megjegyzés

A $\lambda_1 b_1 + \ldots + \lambda_n b_n \mapsto (\lambda_1, \ldots, \lambda_n)$ megfeleltetés nyilván összegtartó. Ezért T additív csoportja izomorf a $\mathbb{Z}_p^+ \times \ldots \times \mathbb{Z}_p^+$ n-tényezős direkt szorzattal.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$,

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d,

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d, akkor e gyökök éppen g hatványai.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d, akkor e gyökök éppen g hatványai.
Speciálisan minden d rendű elem g-nek hatványa!

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d, akkor e gyökök éppen g hatványai.
Speciálisan minden d rendű elem g-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab d rendű elem van.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d, akkor e gyökök éppen g hatványai.
Speciálisan minden d rendű elem g-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab d rendű elem van.
Vagyis a d rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d, akkor e gyökök éppen g hatványai.
Speciálisan minden d rendű elem g-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab d rendű elem van.
Vagyis a d rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs d rendű elem Lagrange tétele miatt.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d, akkor e gyökök éppen g hatványai.
Speciálisan minden d rendű elem g-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab d rendű elem van.
Vagyis a d rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs d rendű elem Lagrange tétele miatt.
Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$-ben a fokokat véve $\sum_{d|k} \varphi(d) = k$.

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d, akkor e gyökök éppen g hatványai.
Speciálisan minden d rendű elem g-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab d rendű elem van.
Vagyis a d rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs d rendű elem Lagrange tétele miatt.
Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$-ben a fokokat véve $\sum_{d|k} \varphi(d) = k$.
Ez csak úgy lehet, ha minden $d \mid k$-ra van d rendű elem!

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d, akkor e gyökök éppen g hatványai.
Speciálisan minden d rendű elem g-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab d rendű elem van.
Vagyis a d rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs d rendű elem Lagrange tétele miatt.
Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$-ben a fokokat véve $\sum_{d|k} \varphi(d) = k$.
Ez csak úgy lehet, ha minden $d \mid k$-ra van d rendű elem!
Speciálisan van k rendű elem,

Véges test multiplikatív csoportja

4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

Bizonyításvázlat

Legyen T elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb d gyöke van T-ben.
Így ha $g \in T^\times$ rendje d, akkor e gyökök éppen g hatványai.
Speciálisan minden d rendű elem g-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab d rendű elem van.
Vagyis a d rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs d rendű elem Lagrange tétele miatt.
Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$-ben a fokokat véve $\sum_{d|k} \varphi(d) = k$.
Ez csak úgy lehet, ha minden $d \mid k$-ra van d rendű elem!
Speciálisan van k rendű elem, azaz $T^\times$ ciklikus. □

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik.

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$.

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest,

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban,

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban,
(hiszen K karakterisztikája p

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban,
(hiszen K karakterisztikája p és $q = p^k$;

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban, (hiszen K karakterisztikája p és $q = p^k$; HF).

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban, (hiszen K karakterisztikája p és $q = p^k$; HF).
Az L elemszáma q,

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban, (hiszen K karakterisztikája p és $q = p^k$; HF).
Az L elemszáma q, mert $x^q - x$-nek nincs többszörös gyöke.

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban, (hiszen K karakterisztikája p és $q = p^k$; HF).
Az L elemszáma q, mert $x^q - x$-nek nincs többszörös gyöke.
Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is.

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban, (hiszen K karakterisztikája p és $q = p^k$; HF).
Az L elemszáma q, mert $x^q - x$-nek nincs többszörös gyöke.
Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is.
De $x^q - x \in \mathbb{Z}_p[x]$ deriváltja $qx^{q-1} - 1 = -1$,

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban, (hiszen K karakterisztikája p és $q = p^k$; HF).
Az L elemszáma q, mert $x^q - x$-nek nincs többszörös gyöke.
Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is.
De $x^q - x \in \mathbb{Z}_p[x]$ deriváltja $qx^{q-1} - 1 = -1$, hiszen $p \mid q$.

Véges test konstrukciója

6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab q elemű test létezik. Jele $\mathbb{F}_q$. Egyértelműség: NB.

Bizonyításvázlat

Legyen K az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (létezik!).
Jelölje L az $x^q - x$ gyökeinek halmazát K-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a K-ban, (hiszen K karakterisztikája p és $q = p^k$; HF).
Az L elemszáma q, mert $x^q - x$-nek nincs többszörös gyöke.
Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is.
De $x^q - x \in \mathbb{Z}_p[x]$ deriváltja $qx^{q-1} - 1 = -1$, hiszen $p \mid q$.
A -1 konstans polinomnak pedig nincs gyöke K-ban. □

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van,

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$,

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.
A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.
A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Lagrange tételét alkalmazzuk az $L^\times$ csoportra.

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.
A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Lagrange tételét alkalmazzuk az $L^\times$ csoportra.
Azt kapjuk, hogy L nem nulla elemei gyökei $x^{p^k-1} - 1$-nek.

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.
A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Lagrange tételét alkalmazzuk az $L^\times$ csoportra.
Azt kapjuk, hogy L nem nulla elemei gyökei $x^{p^k-1} - 1$-nek.
Így L elemei gyökei $x^{p^k} - x$-nek;

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.
A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Lagrange tételét alkalmazzuk az $L^\times$ csoportra.
Azt kapjuk, hogy L nem nulla elemei gyökei $x^{p^k-1} - 1$-nek.
Így L elemei gyökei $x^{p^k} - x$-nek; $|L| = p^k$ miatt több gyök nincs.

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.
A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Lagrange tételét alkalmazzuk az $L^\times$ csoportra.
Azt kapjuk, hogy L nem nulla elemei gyökei $x^{p^k-1} - 1$-nek.
Így L elemei gyökei $x^{p^k} - x$-nek; $|L| = p^k$ miatt több gyök nincs.
Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$.

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.
A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Lagrange tételét alkalmazzuk az $L^\times$ csoportra.
Azt kapjuk, hogy L nem nulla elemei gyökei $x^{p^k-1} - 1$-nek.
Így L elemei gyökei $x^{p^k} - x$-nek; $|L| = p^k$ miatt több gyök nincs.
Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$.

Mivel $L^\times$ ciklikus,

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.
A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Lagrange tételét alkalmazzuk az $L^\times$ csoportra.
Azt kapjuk, hogy L nem nulla elemei gyökei $x^{p^k-1} - 1$-nek.
Így L elemei gyökei $x^{p^k} - x$-nek; $|L| = p^k$ miatt több gyök nincs.
Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$.
Mivel $L^\times$ ciklikus, $x^{p^k-1} - 1$-nek $p^k - 1$ gyöke van L-ben.

Véges test résztestei

6.7.8. Tétel

A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

Bizonyításvázlat

Ha $L \leq \mathbb{F}_q$, akkor $|L| = p^k$, hiszen L karakterisztikája is p.
A szorzástétel miatt $k = |L : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Lagrange tételét alkalmazzuk az $L^\times$ csoportra.
Azt kapjuk, hogy L nem nulla elemei gyökei $x^{p^k-1} - 1$-nek.
Így L elemei gyökei $x^{p^k} - x$-nek; $|L| = p^k$ miatt több gyök nincs.
Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$.
Mivel $L^\times$ ciklikus, $x^{p^k-1} - 1$-nek $p^k - 1$ gyöke van L-ben.
Ezek a nullával együtt p^k elemű résztestet alkotnak. □

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom.

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste,

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus,

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme.

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$,

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik. Ezért az irreducibilis m_α foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis m_α foka $|\mathbb{F}_{p^n} : \mathbb{Z}_p| = n$.
Legyen L az n-edfokú, irreducibilis $f \in \mathbb{Z}_p[x]$ felbontási teste.

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis m_α foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Legyen L az n-edfokú, irreducibilis $f \in \mathbb{Z}_p[x]$ felbontási teste.
Ha $\beta \in L$ gyöke f-nek, akkor $|\,\mathbb{Z}_p(\beta) : \mathbb{Z}_p\,| = n$,

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis m_α foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Legyen L az n-edfokú, irreducibilis $f \in \mathbb{Z}_p[x]$ felbontási teste.
Ha $\beta \in L$ gyöke f-nek, akkor $|\,\mathbb{Z}_p(\beta) : \mathbb{Z}_p\,| = n$, így $|\mathbb{Z}_p(\beta)| = p^n$.

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis m_α foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Legyen L az n-edfokú, irreducibilis $f \in \mathbb{Z}_p[x]$ felbontási teste.
Ha $\beta \in L$ gyöke f-nek, akkor $|\,\mathbb{Z}_p(\beta) : \mathbb{Z}_p\,| = n$, így $|\mathbb{Z}_p(\beta)| = p^n$.
Mivel csak egy p^n elemű résztest van,

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis m_α foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Legyen L az n-edfokú, irreducibilis $f \in \mathbb{Z}_p[x]$ felbontási teste.
Ha $\beta \in L$ gyöke f-nek, akkor $|\,\mathbb{Z}_p(\beta) : \mathbb{Z}_p\,| = n$, így $|\mathbb{Z}_p(\beta)| = p^n$.
Mivel csak egy p^n elemű résztest van, ez f felbontási teste.

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis m_α foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Legyen L az n-edfokú, irreducibilis $f \in \mathbb{Z}_p[x]$ felbontási teste.
Ha $\beta \in L$ gyöke f-nek, akkor $|\,\mathbb{Z}_p(\beta) : \mathbb{Z}_p\,| = n$, így $|\mathbb{Z}_p(\beta)| = p^n$.
Mivel csak egy p^n elemű résztest van, ez f felbontási teste.
Az α közös gyöke f-nek és $x^{p^n} - x$-nek,

Véges test, mint egyszerű bővítés

Állítás (6.7.9, 6.7.10)

Minden p prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis n-edfokú f polinom. Minden ilyen f polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

Bizonyításvázlat

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű α eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis m_α foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Legyen L az n-edfokú, irreducibilis $f \in \mathbb{Z}_p[x]$ felbontási teste.
Ha $\beta \in L$ gyöke f-nek, akkor $|\,\mathbb{Z}_p(\beta) : \mathbb{Z}_p\,| = n$, így $|\mathbb{Z}_p(\beta)| = p^n$.
Mivel csak egy p^n elemű résztest van, ez f felbontási teste.
Az α közös gyöke f-nek és $x^{p^n} - x$-nek, így $f(x) \mid x^{p^n} - x$. □

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött,

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$,

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív,

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$,

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$;

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.
$A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$-nek.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.
$A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$-nek. A másik két gyök $A^2 = x^2 + (x^3+x+1)$

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.
$A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$-nek. A másik két gyök $A^2 = x^2 + (x^3+x+1)$ és $A^4 = x^2 + x + (x^3+x+1)$.

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.
$A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$-nek. A másik két gyök $A^2 = x^2 + (x^3+x+1)$ és $A^4 = x^2 + x + (x^3+x+1)$.
A maradék három elem $Ex^3 + Ex^2 + E$-nek lesz gyöke,

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.
$A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$-nek. A másik két gyök $A^2 = x^2 + (x^3+x+1)$ és $A^4 = x^2 + x + (x^3+x+1)$.
A maradék három elem $Ex^3 + Ex^2 + E$-nek lesz gyöke, ezek $A + E$,

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.
$A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$-nek. A másik két gyök $A^2 = x^2 + (x^3+x+1)$ és $A^4 = x^2 + x + (x^3+x+1)$.
A maradék három elem $Ex^3 + Ex^2 + E$-nek lesz gyöke, ezek $A + E$, $A^2 + E$,

A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A 0 és az 1 minimálpolinomja x és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3 + x + 1$ és $x^3 + x^2 + 1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.
$A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$-nek. A másik két gyök $A^2 = x^2 + (x^3+x+1)$ és $A^4 = x^2 + x + (x^3+x+1)$.
A maradék három elem $Ex^3 + Ex^2 + E$-nek lesz gyöke, ezek $A + E$, $A^2 + E$, $A^2 + A + E$.