Algebra2, alapszint

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
ewkiss@cs.elte.hu

14. előadás

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport.

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport,

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve.

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+$

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+$

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times$

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

(3) $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet!

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

(3) $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet!

(4) $\mathbb{Z}_5^+$ nem részcsoportja $\mathbb{Z}^+$-nak:

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

(3) $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet!

(4) $\mathbb{Z}_5^+$ nem részcsoportja $\mathbb{Z}^+$-nak: $6 = 2 + 4$

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

(3) $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet!

(4) $\mathbb{Z}_5^+$ nem részcsoportja $\mathbb{Z}^+$-nak: $6 = 2 + 4 \neq 2 +_5 4 = 1$.

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

(3) $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet!

(4) $\mathbb{Z}_5^+$ nem részcsoportja $\mathbb{Z}^+$-nak: $6 = 2 + 4 \neq 2 +_5 4 = 1$.

(5) A páros permutációk részcsoportot alkotnak S_n-ben.

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

(3) $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet!

(4) $\mathbb{Z}_5^+$ nem részcsoportja $\mathbb{Z}^+$-nak: $6 = 2 + 4 \neq 2 +_5 4 = 1$.

(5) A páros permutációk részcsoportot alkotnak S_n-ben. Neve alternáló csoport, jele A_n.

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

(3) $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet!

(4) $\mathbb{Z}_5^+$ nem részcsoportja $\mathbb{Z}^+$-nak: $6 = 2 + 4 \neq 2 +_5 4 = 1$.

(5) A páros permutációk részcsoportot alkotnak S_n-ben. Neve alternáló csoport, jele A_n.

(6) A mozgások (forgatások) részcsoport $\mathrm{O}(2)$-ben,

A részcsoport fogalma

2.2.15. Definíció

Legyen G csoport. A $H \subseteq G$ részhalmaz részcsoport, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

(3) $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet!

(4) $\mathbb{Z}_5^+$ nem részcsoportja $\mathbb{Z}^+$-nak: $6 = 2 + 4 \neq 2 +_5 4 = 1$.

(5) A páros permutációk részcsoportot alkotnak S_n-ben. Neve alternáló csoport, jele A_n.

(6) A mozgások (forgatások) részcsoport $\mathrm{O}(2)$-ben, jele $\mathrm{SO}(2)$.

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) H zárt a szorzásra,

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) H zárt a szorzásra,
azaz tetszőleges $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$.

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) H zárt a szorzásra,
azaz tetszőleges $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$.

(2) H tartalmazza G neutrális elemét.

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) H zárt a szorzásra,
azaz tetszőleges $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$.

(2) H tartalmazza G neutrális elemét.

(3) H zárt a G-beli inverzképzésre,

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) H zárt a szorzásra,
azaz tetszőleges $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$.

(2) H tartalmazza G neutrális elemét.

(3) H zárt a G-beli inverzképzésre,
azaz tetszőleges $h \in H$ esetén $h^{-1} \in H$.

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) H zárt a szorzásra,
azaz tetszőleges $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$.

(2) H tartalmazza G neutrális elemét.

(3) H zárt a G-beli inverzképzésre,
azaz tetszőleges $h \in H$ esetén $h^{-1} \in H$.

Állítás (4.4.27. Feladat)

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) H zárt a szorzásra,
azaz tetszőleges $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$.

(2) H tartalmazza G neutrális elemét.

(3) H zárt a G-beli inverzképzésre,
azaz tetszőleges $h \in H$ esetén $h^{-1} \in H$.

Állítás (4.4.27. Feladat)

(1) Részcsoportok metszete is részcsoport.

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) H zárt a szorzásra,
azaz tetszőleges $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$.

(2) H tartalmazza G neutrális elemét.

(3) H zárt a G-beli inverzképzésre,
azaz tetszőleges $h \in H$ esetén $h^{-1} \in H$.

Állítás (4.4.27. Feladat)

(1) Részcsoportok metszete is részcsoport.

(2) Két részcsoport uniója csak akkor részcsoport,

A részcsoport jellemzése

Tétel (2.2.16. Feladat)

Legyen G csoport, melyben a művelet jele $*$.
A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) H zárt a szorzásra,
azaz tetszőleges $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$.

(2) H tartalmazza G neutrális elemét.

(3) H zárt a G-beli inverzképzésre,
azaz tetszőleges $h \in H$ esetén $h^{-1} \in H$.

Állítás (4.4.27. Feladat)

(1) Részcsoportok metszete is részcsoport.

(2) Két részcsoport uniója csak akkor részcsoport,
ha valamelyikük tartalmazza a másikat.

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y komplexusszorzata,

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y komplexusszorzata, és $X^{-1} = \{x^{-1} : x \in X\}$ az X komplexusinverze.

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y komplexusszorzata, és $X^{-1} = \{x^{-1} : x \in X\}$ az X komplexusinverze.

Alterek összege (vektortérben) szintén komplexusösszeg.

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y komplexusszorzata, és $X^{-1} = \{x^{-1} : x \in X\}$ az X komplexusinverze.

Alterek összege (vektortérben) szintén komplexusösszeg.

Tétel (4.4.4. Gyakorlat)

Egy G csoport egy H nem üres részhalmazára ekvivalens:

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y komplexusszorzata, és $X^{-1} = \{x^{-1} : x \in X\}$ az X komplexusinverze.

Alterek összege (vektortérben) szintén komplexusösszeg.

Tétel (4.4.4. Gyakorlat)

Egy G csoport egy H nem üres részhalmazára ekvivalens:

(1) H részcsoport.

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y komplexusszorzata, és $X^{-1} = \{x^{-1} : x \in X\}$ az X komplexusinverze.

Alterek összege (vektortérben) szintén komplexusösszeg.

Tétel (4.4.4. Gyakorlat)

Egy G csoport egy H nem üres részhalmazára ekvivalens:

(1) H részcsoport.

(2) $HH = H^{-1} = H$.

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y komplexusszorzata, és $X^{-1} = \{x^{-1} : x \in X\}$ az X komplexusinverze.

Alterek összege (vektortérben) szintén komplexusösszeg.

Tétel (4.4.4. Gyakorlat)

Egy G csoport egy H nem üres részhalmazára ekvivalens:

(1) H részcsoport.

(2) $HH = H^{-1} = H$.

(3) $HH^{-1} \subseteq H$.

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y komplexusszorzata, és $X^{-1} = \{x^{-1} : x \in X\}$ az X komplexusinverze.

Alterek összege (vektortérben) szintén komplexusösszeg.

Tétel (4.4.4. Gyakorlat)

Egy G csoport egy H nem üres részhalmazára ekvivalens:

(1) H részcsoport.

(2) $HH = H^{-1} = H$.

(3) $HH^{-1} \subseteq H$.

Ha H részcsoport és $h \in H$, akkor $hH = Hh = H$.

Komplexusműveletek

4.4.2. Definíció

Ha X és Y tetszőleges részhalmazai egy G csoportnak, akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y komplexusszorzata, és $X^{-1} = \{x^{-1} : x \in X\}$ az X komplexusinverze.

Alterek összege (vektortérben) szintén komplexusösszeg.

Tétel (4.4.4. Gyakorlat)

Egy G csoport egy H nem üres részhalmazára ekvivalens:

(1) H részcsoport.

(2) $HH = H^{-1} = H$.

(3) $HH^{-1} \subseteq H$.

Ha H részcsoport és $h \in H$, akkor $hH = Hh = H$.

A bizonyítás HF.

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje,

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.
Valódi részcsoport: nem az egész csoport.

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.
Valódi részcsoport: nem az egész csoport.
Triviális részcsoport: az egész csoport,

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.
Valódi részcsoport: nem az egész csoport.
Triviális részcsoport: az egész csoport, és az $\{1\}$ részcsoport.

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.
Valódi részcsoport: nem az egész csoport.
Triviális részcsoport: az egész csoport, és az $\{1\}$ részcsoport.

Prímrendű csoportnak csak két részcsoportja van: a triviálisak.

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.
Valódi részcsoport: nem az egész csoport.
Triviális részcsoport: az egész csoport, és az $\{1\}$ részcsoport.

Prímrendű csoportnak csak két részcsoportja van: a triviálisak.

Bizonyítás

Ha a G csoport elemszáma a p prím,

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.
Valódi részcsoport: nem az egész csoport.
Triviális részcsoport: az egész csoport, és az $\{1\}$ részcsoport.

Prímrendű csoportnak csak két részcsoportja van: a triviálisak.

Bizonyítás

Ha a G csoport elemszáma a p prím, akkor Lagrange tétele miatt minden H részcsoport rendje csak 1 vagy p lehet.

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.
Valódi részcsoport: nem az egész csoport.
Triviális részcsoport: az egész csoport, és az $\{1\}$ részcsoport.

Prímrendű csoportnak csak két részcsoportja van: a triviálisak.

Bizonyítás

Ha a G csoport elemszáma a p prím, akkor Lagrange tétele miatt minden H részcsoport rendje csak 1 vagy p lehet.
Ha $|H| = p$, akkor $H = G$.

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.
Valódi részcsoport: nem az egész csoport.
Triviális részcsoport: az egész csoport, és az $\{1\}$ részcsoport.

Prímrendű csoportnak csak két részcsoportja van: a triviálisak.

Bizonyítás

Ha a G csoport elemszáma a p prím, akkor Lagrange tétele miatt minden H részcsoport rendje csak 1 vagy p lehet.
Ha $|H| = p$, akkor $H = G$. Ha $|H| = 1$, akkor $H = \{1\}$,

Lagrange tétele

Lagrange tétele (4.4.11)

Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának.

Elnevezések: A csoport elemszáma a csoport rendje, jele $|G|$.
Valódi részcsoport: nem az egész csoport.
Triviális részcsoport: az egész csoport, és az $\{1\}$ részcsoport.

Prímrendű csoportnak csak két részcsoportja van: a triviálisak.

Bizonyítás

Ha a G csoport elemszáma a p prím, akkor Lagrange tétele miatt minden H részcsoport rendje csak 1 vagy p lehet.
Ha $|H| = p$, akkor $H = G$. Ha $|H| = 1$, akkor $H = \{1\}$, mert minden részcsoport tartalmazza az egységelemet.

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra.

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma.

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek,

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek, így $|G| = k|H|$,

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek, így $|G| = k|H|$, ahol k ezeknek a részhalmazoknak a száma.

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek, így $|G| = k|H|$, ahol k ezeknek a részhalmazoknak a száma.

4.4.6. Definíció

Ha $H \leq G$ és $g \in G$, akkor

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek, így $|G| = k|H|$, ahol k ezeknek a részhalmazoknak a száma.

4.4.6. Definíció

Ha $H \leq G$ és $g \in G$, akkor $gH = \{gh : h \in H\}$ bal oldali H szerinti mellékosztály.

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek, így $|G| = k|H|$, ahol k ezeknek a részhalmazoknak a száma.

4.4.6. Definíció

Ha $H \leq G$ és $g \in G$, akkor $gH = \{gh : h \in H\}$ bal oldali, $Hg = \{hg : h \in H\}$ jobb oldali H szerinti mellékosztály.

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek, így $|G| = k|H|$, ahol k ezeknek a részhalmazoknak a száma.

4.4.6. Definíció

Ha $H \leq G$ és $g \in G$, akkor $gH = \{gh : h \in H\}$ bal oldali, $Hg = \{hg : h \in H\}$ jobb oldali H szerinti mellékosztály.

Példa

$G = \mathbb{C}^+$, $H = \mathbb{R}^+$.

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek, így $|G| = k|H|$, ahol k ezeknek a részhalmazoknak a száma.

4.4.6. Definíció

Ha $H \leq G$ és $g \in G$, akkor $gH = \{gh : h \in H\}$ bal oldali, $Hg = \{hg : h \in H\}$ jobb oldali H szerinti mellékosztály.

Példa

$G = \mathbb{C}^+$, $H = \mathbb{R}^+$. Ekkor a H szerinti mellékosztályok az x-tengellyel (a valós tengellyel) párhuzamos egyenesek.

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata

Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek, így $|G| = k|H|$, ahol k ezeknek a részhalmazoknak a száma.

4.4.6. Definíció

Ha $H \leq G$ és $g \in G$, akkor $gH = \{gh : h \in H\}$ bal oldali, $Hg = \{hg : h \in H\}$ jobb oldali H szerinti mellékosztály.

Példa

$G = \mathbb{C}^+$, $H = \mathbb{R}^+$. Ekkor a H szerinti mellékosztályok az x-tengellyel (a valós tengellyel) párhuzamos egyenesek. Például $(2+3i)+H = (8+3i)+H$ az $y = 3$ egyenletű egyenes.

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$.

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$,

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás

Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre.

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás

Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre.
Ekkor $aH = bhH$

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás

Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre.
Ekkor $aH = bhH = bH$,

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás

Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre.
Ekkor $aH = bhH = bH$, mert $hH = H$. □

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás

Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre.
Ekkor $aH = bhH = bH$, mert $hH = H$. □

A $hH = H$ bizonyításában felhasználtuk az inverz létezését!

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás

Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre.
Ekkor $aH = bhH = bH$, mert $hH = H$. □

A $hH = H$ bizonyításában felhasználtuk az inverz létezését!

4.4.13. Következmény

Ha cH-nak és dH-nak van közös eleme, akkor egyenlők.

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás

Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre.
Ekkor $aH = bhH = bH$, mert $hH = H$. □

A $hH = H$ bizonyításában felhasználtuk az inverz létezését!

4.4.13. Következmény

Ha cH-nak és dH-nak van közös eleme, akkor egyenlők.

Bizonyítás

Ha $a \in cH \cap dH$,

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás

Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre.
Ekkor $aH = bhH = bH$, mert $hH = H$. □

A $hH = H$ bizonyításában felhasználtuk az inverz létezését!

4.4.13. Következmény

Ha cH-nak és dH-nak van közös eleme, akkor egyenlők.

Bizonyítás

Ha $a \in cH \cap dH$, akkor az előző miatt $cH = aH$

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)

Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás

Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre.
Ekkor $aH = bhH = bH$, mert $hH = H$. □

A $hH = H$ bizonyításában felhasználtuk az inverz létezését!

4.4.13. Következmény

Ha cH-nak és dH-nak van közös eleme, akkor egyenlők.

Bizonyítás

Ha $a \in cH \cap dH$, akkor az előző miatt $cH = aH = dH$. □

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt). Ezért minden mellékosztály elemszáma $|H|$.

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G,

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G, mert $g \in gH$.

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G, mert $g \in gH$.
Az egyenlő mellékosztályok közül csak egyet vegyünk,

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G, mert $g \in gH$.
Az egyenlő mellékosztályok közül csak egyet vegyünk,
ezek páronként diszjunktak.

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G, mert $g \in gH$.
Az egyenlő mellékosztályok közül csak egyet vegyünk, ezek páronként diszjunktak. Ha számuk k, akkor $|G| = k|H|$.

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G, mert $g \in gH$.
Az egyenlő mellékosztályok közül csak egyet vegyünk, ezek páronként diszjunktak. Ha számuk k, akkor $|G| = k|H|$.

4.4.12. Definíció

Ha $H \leq G$, akkor a különböző H szerinti bal mellékosztályok számát a H részcsoport G-beli indexének hívjuk,

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G, mert $g \in gH$.
Az egyenlő mellékosztályok közül csak egyet vegyünk, ezek páronként diszjunktak. Ha számuk k, akkor $|G| = k|H|$.

4.4.12. Definíció

Ha $H \leq G$, akkor a különböző H szerinti bal mellékosztályok számát a H részcsoport G-beli indexének hívjuk, jele $|G : H|$.

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G, mert $g \in gH$.
Az egyenlő mellékosztályok közül csak egyet vegyünk, ezek páronként diszjunktak. Ha számuk k, akkor $|G| = k|H|$.

4.4.12. Definíció

Ha $H \leq G$, akkor a különböző H szerinti bal mellékosztályok számát a H részcsoport G-beli indexének hívjuk, jele $|G : H|$.

Tehát véges csoportban $|G| = |H||G : H|$.

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G, mert $g \in gH$.
Az egyenlő mellékosztályok közül csak egyet vegyünk, ezek páronként diszjunktak. Ha számuk k, akkor $|G| = k|H|$.

4.4.12. Definíció

Ha $H \leq G$, akkor a különböző H szerinti bal mellékosztályok számát a H részcsoport G-beli indexének hívjuk, jele $|G : H|$.

Tehát véges csoportban $|G| = |H||G : H|$.
A bal és jobb mellékosztályok száma megegyezik,

Részcsoport indexe

A Lagrange-tétel bizonyítása

Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt).
Ezért minden mellékosztály elemszáma $|H|$.
A mellékosztályok egyesítése az egész G, mert $g \in gH$.
Az egyenlő mellékosztályok közül csak egyet vegyünk, ezek páronként diszjunktak. Ha számuk k, akkor $|G| = k|H|$.

4.4.12. Definíció

Ha $H \leq G$, akkor a különböző H szerinti bal mellékosztályok számát a H részcsoport G-beli indexének hívjuk, jele $|G : H|$.

Tehát véges csoportban $|G| = |H||G : H|$.
A bal és jobb mellékosztályok száma megegyezik, mert $(gH) \leftrightarrow (gH)^{-1} = Hg^{-1}$ bijektív megfeleltetés (4.4.18. Feladat).

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a *g által generált részcsoport*,

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a g által generált részcsoport, jele $\langle g \rangle$.

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a g által generált részcsoport, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a *g által generált részcsoport*, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény

Minden elem rendje osztója a csoport rendjének,

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a *g által generált részcsoport*, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény

Minden elem rendje osztója a csoport rendjének, így $g^{|G|} = 1$.

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a *g által generált részcsoport*, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény

Minden elem rendje osztója a csoport rendjének, így $g^{|G|} = 1$.

A második állítás igaz, mert $o(g) \Big| |G|$

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a *g által generált részcsoport*, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény

Minden elem rendje osztója a csoport rendjének, így $g^{|G|} = 1$.

A második állítás igaz, mert $o(g) \mid |G|$ miatt $|G|$ jó kitevője g-nek.

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a g által generált részcsoport, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény

Minden elem rendje osztója a csoport rendjének, így $g^{|G|} = 1$.

A második állítás igaz, mert $o(g) \mid |G|$ miatt $|G|$ jó kitevője g-nek.

4.4.21. Következmény

Ebből következik a számelméletben tanult Euler–Fermat-tétel.

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a g által generált részcsoport, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény

Minden elem rendje osztója a csoport rendjének, így $g^{|G|} = 1$.

A második állítás igaz, mert $o(g) \mid |G|$ miatt $|G|$ jó kitevője g-nek.

4.4.21. Következmény

Ebből következik a számelméletben tanult Euler–Fermat-tétel.
$G = \mathbb{Z}_n^\times$,

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a g által generált részcsoport, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény

Minden elem rendje osztója a csoport rendjének, így $g^{|G|} = 1$.

A második állítás igaz, mert $o(g) \mid |G|$ miatt $|G|$ jó kitevője g-nek.

4.4.21. Következmény

Ebből következik a számelméletben tanult Euler–Fermat-tétel.
$G = \mathbb{Z}_n^\times$, ekkor $|G| = \varphi(n)$,

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a g által generált részcsoport, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény

Minden elem rendje osztója a csoport rendjének, így $g^{|G|} = 1$.

A második állítás igaz, mert $o(g) \mid |G|$ miatt $|G|$ jó kitevője g-nek.

4.4.21. Következmény

Ebből következik a számelméletben tanult Euler–Fermat-tétel.
$G = \mathbb{Z}_n^\times$, ekkor $|G| = \varphi(n)$, így ha $(g, n) = 1$,

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)

Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF).
Ez a g által generált részcsoport, jele $\langle g \rangle$.
A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény

Minden elem rendje osztója a csoport rendjének, így $g^{|G|} = 1$.

A második állítás igaz, mert $o(g) \mid |G|$ miatt $|G|$ jó kitevője g-nek.

4.4.21. Következmény

Ebből következik a számelméletben tanult Euler–Fermat-tétel.
$G = \mathbb{Z}_n^\times$, ekkor $|G| = \varphi(n)$, így ha $(g, n) = 1$, akkor $g^{\varphi(n)} \equiv 1\ (n)$.

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport),

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű.

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van.

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van. Tegyük föl, hogy G-nek pontosan két részcsoportja van.

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van. Tegyük föl, hogy G-nek pontosan két részcsoportja van. Ekkor $|G| > 1$,

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van. Tegyük föl, hogy G-nek pontosan két részcsoportja van. Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme.

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van. Tegyük föl, hogy G-nek pontosan két részcsoportja van. Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme. Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$,

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van. Tegyük föl, hogy G-nek pontosan két részcsoportja van. Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme. Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus.

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van.
Tegyük föl, hogy G-nek pontosan két részcsoportja van.
Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme.
Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus.
Nem lehet $G \cong \mathbb{Z}^+$,

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van.
Tegyük föl, hogy G-nek pontosan két részcsoportja van.
Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme.
Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus.
Nem lehet $G \cong \mathbb{Z}^+$, mert itt a páros számok részcsoport.

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van.
Tegyük föl, hogy G-nek pontosan két részcsoportja van.
Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme.
Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus.
Nem lehet $G \cong \mathbb{Z}^+$, mert itt a páros számok részcsoport.
Ha $o(g) = n(\neq 1)$

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van.
Tegyük föl, hogy G-nek pontosan két részcsoportja van.
Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme.
Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus.
Nem lehet $G \cong \mathbb{Z}^+$, mert itt a páros számok részcsoport.
Ha $o(g) = n(\neq 1)$ és p prímosztója n-nek,

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van.
Tegyük föl, hogy G-nek pontosan két részcsoportja van.
Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme.
Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus.
Nem lehet $G \cong \mathbb{Z}^+$, mert itt a páros számok részcsoport.
Ha $o(g) = n(\neq 1)$ és p prímosztója n-nek, akkor

$$h = g^{n/p} \text{ rendje } p.$$

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van.
Tegyük föl, hogy G-nek pontosan két részcsoportja van.
Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme.
Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus.
Nem lehet $G \cong \mathbb{Z}^+$, mert itt a páros számok részcsoport.
Ha $o(g) = n(\neq 1)$ és p prímosztója n-nek, akkor
a hatvány rendjének képlete miatt $h = g^{n/p}$ rendje p.

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű.
Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van.
Tegyük föl, hogy G-nek pontosan két részcsoportja van.
Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme.
Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus.
Nem lehet $G \cong \mathbb{Z}^+$, mert itt a páros számok részcsoport.
Ha $o(g) = n(\neq 1)$ és p prímosztója n-nek, akkor
a hatvány rendjének képlete miatt $h = g^{n/p}$ rendje p.
Így $1 \neq h$ is generálja G-t,

Csoportok kevés részcsoporttal

4.4.23. Tétel

Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás

Láttuk, hogy prímrendű csoportnak csak két részcsoportja van.
Tegyük föl, hogy G-nek pontosan két részcsoportja van.
Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme.
Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus.
Nem lehet $G \cong \mathbb{Z}^+$, mert itt a páros számok részcsoport.
Ha $o(g) = n(\neq 1)$ és p prímosztója n-nek, akkor
a hatvány rendjének képlete miatt $h = g^{n/p}$ rendje p.
Így $1 \neq h$ is generálja G-t, azaz G prímrendű és ciklikus. □

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$,

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.
Ekkor $g^r = g^{k-mq}$

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.
Ekkor $g^r = g^{k-mq} = g^k (g^m)^{-q}$

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.
Ekkor $g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$,

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.
Ekkor $g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$, hiszen $g^k, g^m \in H$.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.
Ekkor $g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$, hiszen $g^k, g^m \in H$.
Mivel m minimális pozitív volt, csak $r = 0$ lehetséges.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.
Ekkor $g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$, hiszen $g^k, g^m \in H$.
Mivel m minimális pozitív volt, csak $r = 0$ lehetséges.
Ezért $g^k = (g^m)^q$,

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.
Ekkor $g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$, hiszen $g^k, g^m \in H$.
Mivel m minimális pozitív volt, csak $r = 0$ lehetséges.
Ezért $g^k = (g^m)^q$, vagyis g^k hatványa g^m-nek.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.
Ekkor $g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$, hiszen $g^k, g^m \in H$.
Mivel m minimális pozitív volt, csak $r = 0$ lehetséges.
Ezért $g^k = (g^m)^q$, vagyis g^k hatványa g^m-nek. Így $H \subseteq \langle g^m \rangle$.

Ciklikus részcsoportja ciklikus

4.3.26. Lemma

Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás

Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus.
Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$.
Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is.
Legyen m a legkisebb pozitív egész, melyre $g^m \in H$.
Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$.
Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$.
Ekkor $g^r = g^{k-mq} = g^k (g^m)^{-q} \in H$, hiszen $g^k, g^m \in H$.
Mivel m minimális pozitív volt, csak $r = 0$ lehetséges.
Ezért $g^k = (g^m)^q$, vagyis g^k hatványa g^m-nek. Így $H \subseteq \langle g^m \rangle$.

Így $\mathbb{Z}^+$ részcsoportjai az m-mel osztható számok minden m-re.

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport,

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik.

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll,

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa,

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás

Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$.

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás

Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$.
Lagrange tétele miatt $(g^k)^d = 1$,

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás

Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$.
Lagrange tétele miatt $(g^k)^d = 1$, azaz $n \mid kd$,

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás

Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$.
Lagrange tétele miatt $(g^k)^d = 1$, azaz $n \mid kd$, így $(n/d) \mid k$.

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás

Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$.
Lagrange tétele miatt $(g^k)^d = 1$, azaz $n \mid kd$, így $(n/d) \mid k$.
Az n/d számnak $0, 1, \ldots, n-1$ között csak d többszöröse van,

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás

Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$.
Lagrange tétele miatt $(g^k)^d = 1$, azaz $n \mid kd$, így $(n/d) \mid k$.
Az n/d számnak $0, 1, \ldots, n-1$ között csak d többszöröse van, ezért H csakis a $g^{n/d}$ elem d darab hatványából állhat.

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás

Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$.
Lagrange tétele miatt $(g^k)^d = 1$, azaz $n \mid kd$, így $(n/d) \mid k$.
Az n/d számnak $0, 1, \ldots, n-1$ között csak d többszöröse van, ezért H csakis a $g^{n/d}$ elem d darab hatványából állhat.
Közben kijött, hogy G minden d rendű eleme H-ban van,

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás

Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$.
Lagrange tétele miatt $(g^k)^d = 1$, azaz $n \mid kd$, így $(n/d) \mid k$.
Az n/d számnak $0, 1, \ldots, n-1$ között csak d többszöröse van, ezért H csakis a $g^{n/d}$ elem d darab hatványából állhat.
Közben kijött, hogy G minden d rendű eleme H-ban van, ezek pont a H generátorelemei. □

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás

Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik.
Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$.
G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás

Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$.
Lagrange tétele miatt $(g^k)^d = 1$, azaz $n \mid kd$, így $(n/d) \mid k$.
Az n/d számnak $0, 1, \ldots, n-1$ között csak d többszöröse van, ezért H csakis a $g^{n/d}$ elem d darab hatványából állhat.
Közben kijött, hogy G minden d rendű eleme H-ban van, ezek pont a H generátorelemei. □

Ezzel elvégeztük a 4.3. és a 4.4. szakaszt.