Algebra3, alkalmazott matematikus

ELTE Algebra és Számelmélet Tanszék

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

4/11. előadás

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként” végezzük.

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként” végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként” végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal” dolgozni.

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként” végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal” dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok,

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként” végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal” dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$
a $(g_1, \ldots, g_n)$ sorozatok halmaza,

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként” végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal” dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$ a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként” végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal” dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$ a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként” végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal” dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$ a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

(az i-edik komponensben a G_i csoport szorzását végezzük).

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként" végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal" dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$ a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

(az i-edik komponensben a G_i csoport szorzását végezzük).
Egységelem: $(e_1, \ldots, e_n)$,

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként" végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal" dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$
a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

(az i-edik komponensben a G_i csoport szorzását végezzük).
Egységelem: $(e_1, \ldots, e_n)$, ahol e_i a G_i egységeleme.

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként" végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal" dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$ a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

(az i-edik komponensben a G_i csoport szorzását végezzük).
Egységelem: $(e_1, \ldots, e_n)$, ahol e_i a G_i egységeleme.
Inverz: $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként" végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal" dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$
a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

(az i-edik komponensben a G_i csoport szorzását végezzük).
Egységelem: $(e_1, \ldots, e_n)$, ahol e_i a G_i egységeleme.
Inverz: $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$ (komponensenként).

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként" végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal" dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$ a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

(az i-edik komponensben a G_i csoport szorzását végezzük).
Egységelem: $(e_1, \ldots, e_n)$, ahol e_i a G_i egységeleme.
Inverz: $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$ (komponensenként).
Asszociativitás: HF.

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként" végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal" dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$
a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

(az i-edik komponensben a G_i csoport szorzását végezzük).
Egységelem: $(e_1, \ldots, e_n)$, ahol e_i a G_i egységeleme.
Inverz: $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$ (komponensenként).
Asszociativitás: HF. Tehát csoportot kaptunk.

A direkt szorzat fogalma

Az n magas oszlopvektorok vektorteret alkotnak.
Ebben a műveletet „komponensenként" végezzük.
Ezt akkor is megtehetjük, ha a komponensek csoportelemek.
Kényelmesebb lesz „sorvektorokkal" dolgozni.

4.9.2. Definíció

Legyenek $G_1, \ldots, G_n$ csoportok, és $G_1 \times \ldots \times G_n$
a $(g_1, \ldots, g_n)$ sorozatok halmaza, ahol $g_i \in G_i$ minden i-re.

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

(az i-edik komponensben a G_i csoport szorzását végezzük).
Egységelem: $(e_1, \ldots, e_n)$, ahol e_i a G_i egységeleme.
Inverz: $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$ (komponensenként).
Asszociativitás: HF. Tehát csoportot kaptunk.
Ez a $G_1, \ldots, G_n$ csoportok direkt szorzata.

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2, 3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2, 3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2, 3)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2, 3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2, 3)$, $g^2 = (4, 4)$, $g^3 = (8, 2)$, $g^4 = (7, 1)$,
$g^5 = (5, 3)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$, $g^7 = (2,2)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$, $g^7 = (2,2)$, $g^8 = (4,1)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$, $g^7 = (2,2)$, $g^8 = (4,1)$,
$g^9 = (8,3)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2, 3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2, 3)$, $g^2 = (4, 4)$, $g^3 = (8, 2)$, $g^4 = (7, 1)$,
$g^5 = (5, 3)$, $g^6 = (1, 4)$, $g^7 = (2, 2)$, $g^8 = (4, 1)$,
$g^9 = (8, 3)$, $g^{10} = (7, 4)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$, $g^7 = (2,2)$, $g^8 = (4,1)$,
$g^9 = (8,3)$, $g^{10} = (7,4)$, $g^{11} = (5,2)$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?

$$\begin{aligned}
g^1 &= (2,3), & g^2 &= (4,4), & g^3 &= (8,2), & g^4 &= (7,1),\\
g^5 &= (5,3), & g^6 &= (1,4), & g^7 &= (2,2), & g^8 &= (4,1),\\
g^9 &= (8,3), & g^{10} &= (7,4), & g^{11} &= (5,2), & g^{12} &= (1,1).
\end{aligned}$$

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$, $g^7 = (2,2)$, $g^8 = (4,1)$,
$g^9 = (8,3)$, $g^{10} = (7,4)$, $g^{11} = (5,2)$, $g^{12} = (1,1)$.
Vagyis g rendje 12.

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?

$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$, $g^7 = (2,2)$, $g^8 = (4,1)$,
$g^9 = (8,3)$, $g^{10} = (7,4)$, $g^{11} = (5,2)$, $g^{12} = (1,1)$.

Vagyis g rendje 12. De $o_9(2) = 6$,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$, $g^7 = (2,2)$, $g^8 = (4,1)$,
$g^9 = (8,3)$, $g^{10} = (7,4)$, $g^{11} = (5,2)$, $g^{12} = (1,1)$.
Vagyis g rendje 12. De $o_9(2) = 6$, $o_5(3) = 4$

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$, $g^7 = (2,2)$, $g^8 = (4,1)$,
$g^9 = (8,3)$, $g^{10} = (7,4)$, $g^{11} = (5,2)$, $g^{12} = (1,1)$.
Vagyis g rendje 12. De $o_9(2) = 6$, $o_5(3) = 4$ és $12 = [6,4]$.

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?

$$\begin{aligned} g^1 &= (2,3), & g^2 &= (4,4), & g^3 &= (8,2), & g^4 &= (7,1), \\ g^5 &= (5,3), & g^6 &= (1,4), & g^7 &= (2,2), & g^8 &= (4,1), \\ g^9 &= (8,3), & g^{10} &= (7,4), & g^{11} &= (5,2), & g^{12} &= (1,1). \end{aligned}$$

Vagyis g rendje 12. De $o_9(2) = 6$, $o_5(3) = 4$ és $12 = [6,4]$.

4.9.4. Állítás (bizonyítás HF)

Egy direkt szorzat tetszőleges elemének rendje
a komponensei rendjeinek legkisebb közös többszöröse,

Példák direkt szorzatra

A sík vektorai az összeadásra éppen $\mathbb{R}^+ \times \mathbb{R}^+$.
Ugyanígy $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$, hiszen $\mathbb{C}$ elemeit ugyanúgy kell összeadni, mint a síkvektorokat.

Mi lesz $g = (2,3)$ rendje $\mathbb{Z}_9^\times \times \mathbb{Z}_5^\times$-ben?

$$\begin{aligned} g^1 &= (2,3), & g^2 &= (4,4), & g^3 &= (8,2), & g^4 &= (7,1), \\ g^5 &= (5,3), & g^6 &= (1,4), & g^7 &= (2,2), & g^8 &= (4,1), \\ g^9 &= (8,3), & g^{10} &= (7,4), & g^{11} &= (5,2), & g^{12} &= (1,1). \end{aligned}$$

Vagyis g rendje 12. De $o_9(2) = 6$, $o_5(3) = 4$ és $12 = [6,4]$.

4.9.4. Állítás (bizonyítás HF)

Egy direkt szorzat tetszőleges elemének rendje a komponensei rendjeinek legkisebb közös többszöröse, illetve végtelen, ha a komponensek között van végtelen rendű.

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1, 1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1, 1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1, 1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3.

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1, 1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2, 3] = 6$.

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6.

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1, 1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2, 3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport,

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport, és így

$$\mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+.$$

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport, és így

$$\mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+ .$$

4.9.8. Következmény (bizonyítás hasonlóan)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \cong \mathbb{Z}_{nm}^+$.

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport, és így

$$\mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+ .$$

4.9.8. Következmény (bizonyítás hasonlóan)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \cong \mathbb{Z}_{nm}^+$.

Ugyanígy több tényezőre,

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport, és így

$$\mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+.$$

4.9.8. Következmény (bizonyítás hasonlóan)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \cong \mathbb{Z}_{nm}^+$.

Ugyanígy több tényezőre, pl. $\mathbb{Z}_{60}^+ \cong \mathbb{Z}_4^+ \times \mathbb{Z}_3^+ \times \mathbb{Z}_5^+$.

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport, és így

$$\mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+ .$$

4.9.8. Következmény (bizonyítás hasonlóan)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \cong \mathbb{Z}_{nm}^+$.

Ugyanígy több tényezőre, pl. $\mathbb{Z}_{60}^+ \cong \mathbb{Z}_4^+ \times \mathbb{Z}_3^+ \times \mathbb{Z}_5^+$. Megfordítás:

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport, és így

$$\mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+ .$$

4.9.8. Következmény (bizonyítás hasonlóan)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \cong \mathbb{Z}_{nm}^+$.

Ugyanígy több tényezőre, pl. $\mathbb{Z}_{60}^+ \cong \mathbb{Z}_4^+ \times \mathbb{Z}_3^+ \times \mathbb{Z}_5^+$. Megfordítás:

4.9.8. Következmény (HF)

Ha $G \times H$ véges ciklikus csoport,

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport, és így

$$\mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+ .$$

4.9.8. Következmény (bizonyítás hasonlóan)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \cong \mathbb{Z}_{nm}^+$.

Ugyanígy több tényezőre, pl. $\mathbb{Z}_{60}^+ \cong \mathbb{Z}_4^+ \times \mathbb{Z}_3^+ \times \mathbb{Z}_5^+$. Megfordítás:

4.9.8. Következmény (HF)

Ha $G \times H$ véges ciklikus csoport, akkor G és H is ciklikus,

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport, és így

$$\mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+ .$$

4.9.8. Következmény (bizonyítás hasonlóan)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \cong \mathbb{Z}_{nm}^+$.

Ugyanígy több tényezőre, pl. $\mathbb{Z}_{60}^+ \cong \mathbb{Z}_4^+ \times \mathbb{Z}_3^+ \times \mathbb{Z}_5^+$. Megfordítás:

4.9.8. Következmény (HF)

Ha $G \times H$ véges ciklikus csoport, akkor G és H is ciklikus, és rendjük relatív prím.

Ciklikus csoportok direkt felbontása

Mi lesz $g = (1,1)$ rendje $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$-ban?
1 rendje $\mathbb{Z}_2^+$-ban 2 és 1 rendje $\mathbb{Z}_3^+$-ban 3. Így $o(g) = [2,3] = 6$.
De $\mathbb{Z}_2^+ \times \mathbb{Z}_3^+$ rendje is 6. Ezért ez ciklikus csoport, és így

$$\mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+ .$$

4.9.8. Következmény (bizonyítás hasonlóan)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \cong \mathbb{Z}_{nm}^+$.

Ugyanígy több tényezőre, pl. $\mathbb{Z}_{60}^+ \cong \mathbb{Z}_4^+ \times \mathbb{Z}_3^+ \times \mathbb{Z}_5^+$. Megfordítás:

4.9.8. Következmény (HF)

Ha $G \times H$ véges ciklikus csoport, akkor G és H is ciklikus, és rendjük relatív prím.

Ötlet: $G \times H$-nak van G-vel izomorf részcsoportja (és faktora is).

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n,

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n, ha hatványai kiadják az összes redukált maradékosztályt mod n.

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n, ha hatványai kiadják az összes redukált maradékosztályt mod n.
Vagyis a primitív gyökök a $\mathbb{Z}_n^\times$ csoport generátorelemei.

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n, ha hatványai kiadják az összes redukált maradékosztályt mod n.
Vagyis a primitív gyökök a $\mathbb{Z}_n^\times$ csoport generátorelemei.

Tétel

Pontosan akkor létezik primitív gyök mod n,

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n, ha hatványai kiadják az összes redukált maradékosztályt mod n.
Vagyis a primitív gyökök a $\mathbb{Z}_n^\times$ csoport generátorelemei.

Tétel

Pontosan akkor létezik primitív gyök mod n, ha $n = 1, 2, 4,$

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n, ha hatványai kiadják az összes redukált maradékosztályt mod n.
Vagyis a primitív gyökök a $\mathbb{Z}_n^\times$ csoport generátorelemei.

Tétel

Pontosan akkor létezik primitív gyök mod n, ha $n = 1, 2, 4$, vagy egy páratlan prímhatvány,

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n, ha hatványai kiadják az összes redukált maradékosztályt mod n.
Vagyis a primitív gyökök a $\mathbb{Z}_n^\times$ csoport generátorelemei.

Tétel

Pontosan akkor létezik primitív gyök mod n, ha $n = 1, 2, 4$, vagy egy páratlan prímhatvány, vagy annak kétszerese.

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n, ha hatványai kiadják az összes redukált maradékosztályt mod n.
Vagyis a primitív gyökök a $\mathbb{Z}_n^\times$ csoport generátorelemei.

Tétel

Pontosan akkor létezik primitív gyök mod n, ha $n = 1, 2, 4$, vagy egy páratlan prímhatvány, vagy annak kétszerese.

Lásd a jegyzetben: 4.9.10, 4.4.33, 4.9.36.

A $\mathbb{Z}_n^\times$ csoportok direkt felbontása

E.4.4. Tétel (Függelék)

Ha m és n relatív prímek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.

A bizonyítást lásd a jegyzetben, a vizsgára tudni kell.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n, ha hatványai kiadják az összes redukált maradékosztályt mod n.
Vagyis a primitív gyökök a $\mathbb{Z}_n^\times$ csoport generátorelemei.

Tétel

Pontosan akkor létezik primitív gyök mod n, ha $n = 1, 2, 4$, vagy egy páratlan prímhatvány, vagy annak kétszerese.

Lásd a jegyzetben: 4.9.10, 4.4.33, 4.9.36. A vizsgára csak a következő speciális eset bizonyítását kell tudni.

Szükséges feltétel primitív gyök létezésére

4.9.10. Gyakorlat

Ha létezik primitív gyök modulo n, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.

Szükséges feltétel primitív gyök létezésére

4.9.10. Gyakorlat

Ha létezik primitív gyök modulo n, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.

Bizonyítás

Tudjuk, hogy ciklikus csoportok direkt szorzata csak akkor lehet ciklikus, ha rendjeik relatív prímek.

Szükséges feltétel primitív gyök létezésére

4.9.10. Gyakorlat

Ha létezik primitív gyök modulo n, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.

Bizonyítás

Tudjuk, hogy ciklikus csoportok direkt szorzata csak akkor lehet ciklikus, ha rendjeik relatív prímek.
Legyen n a $q_1, \ldots, q_k$ páronként relatív prím (1-nél nagyobb) prímhatványok szorzata.

Szükséges feltétel primitív gyök létezésére

4.9.10. Gyakorlat

Ha létezik primitív gyök modulo n, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.

Bizonyítás

Tudjuk, hogy ciklikus csoportok direkt szorzata csak akkor lehet ciklikus, ha rendjeik relatív prímek.
Legyen n a $q_1, \ldots, q_k$ páronként relatív prím (1-nél nagyobb) prímhatványok szorzata. Láttuk, hogy $\mathbb{Z}_n^\times \cong \mathbb{Z}_{q_1}^\times \times \ldots \times \mathbb{Z}_{q_k}^\times$.

Szükséges feltétel primitív gyök létezésére

4.9.10. Gyakorlat

Ha létezik primitív gyök modulo n, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.

Bizonyítás

Tudjuk, hogy ciklikus csoportok direkt szorzata csak akkor lehet ciklikus, ha rendjeik relatív prímek.
Legyen n a $q_1, \ldots, q_k$ páronként relatív prím (1-nél nagyobb) prímhatványok szorzata. Láttuk, hogy $\mathbb{Z}_n^\times \cong \mathbb{Z}_{q_1}^\times \times \ldots \times \mathbb{Z}_{q_k}^\times$.
Ha $q_i = p^m$ (p prím), akkor $\mathbb{Z}_{q_i}^\times$ rendje $\varphi(q_i) = (p-1)p^{m-1}$.

Szükséges feltétel primitív gyök létezésére

4.9.10. Gyakorlat

Ha létezik primitív gyök modulo n, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.

Bizonyítás

Tudjuk, hogy ciklikus csoportok direkt szorzata csak akkor lehet ciklikus, ha rendjeik relatív prímek.
Legyen n a $q_1, \ldots, q_k$ páronként relatív prím (1-nél nagyobb) prímhatványok szorzata. Láttuk, hogy $\mathbb{Z}_n^\times \cong \mathbb{Z}_{q_1}^\times \times \ldots \times \mathbb{Z}_{q_k}^\times$.
Ha $q_i = p^m$ (p prím), akkor $\mathbb{Z}_{q_i}^\times$ rendje $\varphi(q_i) = (p-1)p^{m-1}$.
Ez csak akkor lehet páratlan, ha $p = 2$ és $m = 1$, azaz $q_i = 2$.

Szükséges feltétel primitív gyök létezésére

4.9.10. Gyakorlat

Ha létezik primitív gyök modulo n, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.

Bizonyítás

Tudjuk, hogy ciklikus csoportok direkt szorzata csak akkor lehet ciklikus, ha rendjeik relatív prímek.
Legyen n a $q_1, \ldots, q_k$ páronként relatív prím (1-nél nagyobb) prímhatványok szorzata. Láttuk, hogy $\mathbb{Z}_n^\times \cong \mathbb{Z}_{q_1}^\times \times \ldots \times \mathbb{Z}_{q_k}^\times$.
Ha $q_i = p^m$ (p prím), akkor $\mathbb{Z}_{q_i}^\times$ rendje $\varphi(q_i) = (p-1)p^{m-1}$.
Ez csak akkor lehet páratlan, ha $p = 2$ és $m = 1$, azaz $q_i = 2$.
A páronként relatív prím $\varphi(q_i)$ számok közül csak egy lehet páros.

Szükséges feltétel primitív gyök létezésére

4.9.10. Gyakorlat

Ha létezik primitív gyök modulo n, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.

Bizonyítás

Tudjuk, hogy ciklikus csoportok direkt szorzata csak akkor lehet ciklikus, ha rendjeik relatív prímek.
Legyen n a $q_1, \ldots, q_k$ páronként relatív prím (1-nél nagyobb) prímhatványok szorzata. Láttuk, hogy $\mathbb{Z}_n^\times \cong \mathbb{Z}_{q_1}^\times \times \ldots \times \mathbb{Z}_{q_k}^\times$.
Ha $q_i = p^m$ (p prím), akkor $\mathbb{Z}_{q_i}^\times$ rendje $\varphi(q_i) = (p-1)p^{m-1}$.
Ez csak akkor lehet páratlan, ha $p = 2$ és $m = 1$, azaz $q_i = 2$.
A páronként relatív prím $\varphi(q_i)$ számok közül csak egy lehet páros.
Ezért legfeljebb két q_i lehet,

Szükséges feltétel primitív gyök létezésére

4.9.10. Gyakorlat

Ha létezik primitív gyök modulo n, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.

Bizonyítás

Tudjuk, hogy ciklikus csoportok direkt szorzata csak akkor lehet ciklikus, ha rendjeik relatív prímek.
Legyen n a $q_1, \ldots, q_k$ páronként relatív prím (1-nél nagyobb) prímhatványok szorzata. Láttuk, hogy $\mathbb{Z}_n^\times \cong \mathbb{Z}_{q_1}^\times \times \ldots \times \mathbb{Z}_{q_k}^\times$.
Ha $q_i = p^m$ (p prím), akkor $\mathbb{Z}_{q_i}^\times$ rendje $\varphi(q_i) = (p-1)p^{m-1}$.
Ez csak akkor lehet páratlan, ha $p = 2$ és $m = 1$, azaz $q_i = 2$.
A páronként relatív prím $\varphi(q_i)$ számok közül csak egy lehet páros.
Ezért legfeljebb két q_i lehet, és ha kettő van, akkor az egyik 2-vel egyenlő. $\square$

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára.

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak.

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait,

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

Példa

Hány 24 elemű Abel-csoport létezik (izomorfia erejéig)?

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

Példa

Hány 24 elemű Abel-csoport létezik (izomorfia erejéig)?

A lehetséges tényezők rendjei a 24 szám prímhatványosztói,

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

Példa

Hány 24 elemű Abel-csoport létezik (izomorfia erejéig)?

A lehetséges tényezők rendjei a 24 szám prímhatványosztói, azaz $2, 4, 8, 3$.

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

Példa

Hány 24 elemű Abel-csoport létezik (izomorfia erejéig)?

A lehetséges tényezők rendjei a 24 szám prímhatványosztói, azaz $2, 4, 8, 3$. Ilyen elemszámú tényezőkből kell a 24-et kikombinálni.

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

Példa

Hány 24 elemű Abel-csoport létezik (izomorfia erejéig)?

A lehetséges tényezők rendjei a 24 szám prímhatványosztói, azaz $2, 4, 8, 3$. Ilyen elemszámú tényezőkből kell a 24-et kikombinálni. A lehetőségek a következők:

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

Példa

Hány 24 elemű Abel-csoport létezik (izomorfia erejéig)?

A lehetséges tényezők rendjei a 24 szám prímhatványosztói, azaz $2, 4, 8, 3$. Ilyen elemszámú tényezőkből kell a 24-et kikombinálni. A lehetőségek a következők:

$$\mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ ,$$

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

Példa

Hány 24 elemű Abel-csoport létezik (izomorfia erejéig)?

A lehetséges tényezők rendjei a 24 szám prímhatványosztói, azaz $2, 4, 8, 3$. Ilyen elemszámú tényezőkből kell a 24-et kikombinálni. A lehetőségek a következők:

$$\mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ , \qquad \mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_4^+ ,$$

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

Példa

Hány 24 elemű Abel-csoport létezik (izomorfia erejéig)?

A lehetséges tényezők rendjei a 24 szám prímhatványosztói, azaz $2, 4, 8, 3$. Ilyen elemszámú tényezőkből kell a 24-et kikombinálni. A lehetőségek a következők:

$$\mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ , \quad \mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_4^+ , \quad \mathbb{Z}_3^+ \times \mathbb{Z}_8^+ .$$

A véges Abel-csoportok alaptétele

4.9.15. Tétel (NB)

Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A tényezők rendjei a sorrendtől eltekintve egyértelműen meghatározottak. Azaz ha nézzük G ilyen felbontásait, akkor minden q prímhatványra a q rendű tényezők száma mindegyik felbontásban ugyanannyi.

Példa

Hány 24 elemű Abel-csoport létezik (izomorfia erejéig)?

A lehetséges tényezők rendjei a 24 szám prímhatványosztói, azaz $2, 4, 8, 3$. Ilyen elemszámú tényezőkből kell a 24-et kikombinálni. A lehetőségek a következők:

$$\mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ , \quad \mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_4^+ , \quad \mathbb{Z}_3^+ \times \mathbb{Z}_8^+ .$$

Így izomorfia erejéig 3 darab 24 rendű Abel-csoport van.

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$.

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok,
ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^*$

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) \ : \ a \in A\}$

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) : a \in A\} = A \times \{1_B\}$;

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) : a \in A\} = A \times \{1_B\}$;
Legyen $\mathrm{Ker}(\pi_1) = B^*$

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) : a \in A\} = A \times \{1_B\}$;
Legyen $\mathrm{Ker}(\pi_1) = B^* = \{(1_A, b) : b \in B\}$

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) : a \in A\} = A \times \{1_B\}$;
Legyen $\mathrm{Ker}(\pi_1) = B^* = \{(1_A, b) : b \in B\} = \{1_A\} \times B$.

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) : a \in A\} = A \times \{1_B\}$;
Legyen $\mathrm{Ker}(\pi_1) = B^* = \{(1_A, b) : b \in B\} = \{1_A\} \times B$.
Ezek tehát normálosztók $A \times B$-ben.

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) : a \in A\} = A \times \{1_B\}$;
Legyen $\mathrm{Ker}(\pi_1) = B^* = \{(1_A, b) : b \in B\} = \{1_A\} \times B$.
Ezek tehát normálosztók $A \times B$-ben.
A homomorfizmustétel miatt $(A \times B)/A^* \cong B$

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) \ : \ a \in A\} = A \times \{1_B\}$;
Legyen $\mathrm{Ker}(\pi_1) = B^* = \{(1_A, b) \ : \ b \in B\} = \{1_A\} \times B$.
Ezek tehát normálosztók $A \times B$-ben.
A homomorfizmustétel miatt $(A \times B)/A^* \cong B$ és $(A \times B)/B^* \cong A$.

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) : a \in A\} = A \times \{1_B\}$;
Legyen $\mathrm{Ker}(\pi_1) = B^* = \{(1_A, b) : b \in B\} = \{1_A\} \times B$.
Ezek tehát normálosztók $A \times B$-ben.
A homomorfizmustétel miatt $(A \times B)/A^* \cong B$ és $(A \times B)/B^* \cong A$.
Nyilván $A^* \cap B^* = (1_A, 1_B)$.

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) : a \in A\} = A \times \{1_B\}$;
Legyen $\mathrm{Ker}(\pi_1) = B^* = \{(1_A, b) : b \in B\} = \{1_A\} \times B$.
Ezek tehát normálosztók $A \times B$-ben.
A homomorfizmustétel miatt $(A \times B)/A^* \cong B$ és $(A \times B)/B^* \cong A$.
Nyilván $A^* \cap B^* = (1_A, 1_B)$.
Továbbá $A^* B^* = A \times B$,

A projekciók és magjaik

Az $A \times B$ direkt szorzat elemei az összes (a, b) párok, ahol $a \in A$ és $b \in B$. Szorzás: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Legyen $\pi_1 : A \times B \to A$, ahol $\pi_1 : (a, b) \mapsto a$.
Legyen $\pi_2 : A \times B \to B$, ahol $\pi_2 : (a, b) \mapsto b$.
Ez a két projekció (homomorfizmus).

4.9.11. Állítás

Legyen $\mathrm{Ker}(\pi_2) = A^* = \{(a, 1_B) \; : \; a \in A\} = A \times \{1_B\}$;
Legyen $\mathrm{Ker}(\pi_1) = B^* = \{(1_A, b) \; : \; b \in B\} = \{1_A\} \times B$.
Ezek tehát normálosztók $A \times B$-ben.
A homomorfizmustétel miatt $(A \times B)/A^* \cong B$ és $(A \times B)/B^* \cong A$.
Nyilván $A^* \cap B^* = (1_A, 1_B)$.
Továbbá $A^* B^* = A \times B$, mert $(a, b) = (a, 1_B)(1_A, b)$.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$,

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$,

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra,

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra, így $aba^{-1} \in B$.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra, így $aba^{-1} \in B$. Mivel B részcsoport, zárt az inverzképzésre és a szorzásra,

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra, így $aba^{-1} \in B$. Mivel B részcsoport, zárt az inverzképzésre és a szorzásra, így $b^{-1} \in B$

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra, így $aba^{-1} \in B$. Mivel B részcsoport, zárt az inverzképzésre és a szorzásra, így $b^{-1} \in B$ és $g \in B$.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra, így $aba^{-1} \in B$. Mivel B részcsoport, zárt az inverzképzésre és a szorzásra, így $b^{-1} \in B$ és $g \in B$. A $g = a(ba^{-1}b^{-1})$ felírásból ugyanígy $g \in A$.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra, így $aba^{-1} \in B$. Mivel B részcsoport, zárt az inverzképzésre és a szorzásra, így $b^{-1} \in B$ és $g \in B$.
A $g = a(ba^{-1}b^{-1})$ felírásból ugyanígy $g \in A$.
Tehát $g \in A \cap B = \{1\}$,

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra, így $aba^{-1} \in B$. Mivel B részcsoport, zárt az inverzképzésre és a szorzásra, így $b^{-1} \in B$ és $g \in B$. A $g = a(ba^{-1}b^{-1})$ felírásból ugyanígy $g \in A$. Tehát $g \in A \cap B = \{1\}$, vagyis $1 = g = aba^{-1}b^{-1}$.

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet. Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra, így $aba^{-1} \in B$. Mivel B részcsoport, zárt az inverzképzésre és a szorzásra, így $b^{-1} \in B$ és $g \in B$. A $g = a(ba^{-1}b^{-1})$ felírásból ugyanígy $g \in A$. Tehát $g \in A \cap B = \{1\}$, vagyis $1 = g = aba^{-1}b^{-1}$. Innen b-vel, majd a-val jobbról szorozva $ba = ab$. $\square$

Felcserélhető elemek

4.8.25. Gyakorlat

Ha A, B normálosztók egy csoportban és $A \cap B = \{1\}$, akkor A minden eleme felcserélhető B minden elemével.

Bizonyítás

Legyen $a \in A$ és $b \in B$. Tekintsük a $g = aba^{-1}b^{-1}$ elemet.
Belátjuk, hogy $g \in B$. Nyilván $g = (aba^{-1})b^{-1}$, itt aba^{-1} a b-nek a-val vett konjugáltja. A B normálosztó zárt a konjugálásra, így $aba^{-1} \in B$. Mivel B részcsoport, zárt az inverzképzésre és a szorzásra, így $b^{-1} \in B$ és $g \in B$.
A $g = a(ba^{-1}b^{-1})$ felírásból ugyanígy $g \in A$.
Tehát $g \in A \cap B = \{1\}$, vagyis $1 = g = aba^{-1}b^{-1}$.
Innen b-vel, majd a-val jobbról szorozva $ba = ab$. $\square$

$[a, b] = aba^{-1}b^{-1}$ az a és b elemek kommutátora.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű:

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$,

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak,

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$,

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$,

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$, és $b = b'$.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$, és $b = b'$.
Így a $\varphi : (a, b) \mapsto ab$ leképezés bijekció $A \times B$ és G között.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$, és $b = b'$.
Így a $\varphi : (a, b) \mapsto ab$ leképezés bijekció $A \times B$ és G között.
Kell: φ szorzattartó.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$, és $b = b'$.
Így a $\varphi : (a, b) \mapsto ab$ leképezés bijekció $A \times B$ és G között.
Kell: φ szorzattartó. Láttuk, hogy $A \cap B = \{1\}$ miatt A elemei fölcserélhetők B elemeivel.

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$, és $b = b'$.
Így a $\varphi : (a, b) \mapsto ab$ leképezés bijekció $A \times B$ és G között.
Kell: φ szorzattartó. Láttuk, hogy $A \cap B = \{1\}$ miatt A elemei fölcserélhetők B elemeivel. Ha $a, a' \in A$ és $b, b' \in B$, akkor $a'b = ba'$,

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$, és $b = b'$.
Így a $\varphi : (a, b) \mapsto ab$ leképezés bijekció $A \times B$ és G között.
Kell: φ szorzattartó. Láttuk, hogy $A \cap B = \{1\}$ miatt A elemei fölcserélhetők B elemeivel. Ha $a, a' \in A$ és $b, b' \in B$, akkor $a'b = ba'$, így $\varphi\big((a, b)(a', b')\big) = \varphi\big((aa', bb')\big)$

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$, és $b = b'$.
Így a $\varphi : (a, b) \mapsto ab$ leképezés bijekció $A \times B$ és G között.
Kell: φ szorzattartó. Láttuk, hogy $A \cap B = \{1\}$ miatt A elemei fölcserélhetők B elemeivel. Ha $a, a' \in A$ és $b, b' \in B$, akkor $a'b = ba'$, így $\varphi\big((a, b)(a', b')\big) = \varphi\big((aa', bb')\big) = aa'bb' =$

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$, és $b = b'$.
Így a $\varphi : (a, b) \mapsto ab$ leképezés bijekció $A \times B$ és G között.
Kell: φ szorzattartó. Láttuk, hogy $A \cap B = \{1\}$ miatt A elemei fölcserélhetők B elemeivel. Ha $a, a' \in A$ és $b, b' \in B$, akkor $a'b = ba'$, így $\varphi((a, b)(a', b')) = \varphi((aa', bb')) = aa'bb' =$
$= aba'b'$

Direkt felbontás keresése

4.9.12. Tétel

Legyen G csoport, és A, B normálosztók G-ben úgy, hogy $A \cap B = \{1\}$ és $AB = G$. Ekkor $G \cong A \times B$.

Bizonyítás

G minden eleme előáll ab alakban, ahol $a \in A$ és $b \in B$.
Ez egyértelmű: ha $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor $a'^{-1}a = b'b^{-1} =: g$. A bal oldal A-nak, a jobb B-nek eleme.
Tehát $g \in A \cap B = \{1\}$, ezért $a'^{-1}a = 1$ miatt $a = a'$, és $b = b'$.
Így a $\varphi : (a, b) \mapsto ab$ leképezés bijekció $A \times B$ és G között.
Kell: φ szorzattartó. Láttuk, hogy $A \cap B = \{1\}$ miatt A elemei fölcserélhetők B elemeivel. Ha $a, a' \in A$ és $b, b' \in B$, akkor $a'b = ba'$, így $\varphi((a, b)(a', b')) = \varphi((aa', bb')) = aa'bb' = $
$= aba'b' = \varphi((a, b))\varphi((a', b'))$. $\square$

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek,

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek, akkor a sík (additív csoportja) nem lesz $e \oplus f \oplus g$.

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek,
akkor a sík (additív csoportja) nem lesz $e \oplus f \oplus g$.

4.9.14. Gyakorlat

A G csoport akkor és csak akkor izomorf $A \times B \times C$-vel,

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek, akkor a sík (additív csoportja) nem lesz $e \oplus f \oplus g$.

4.9.14. Gyakorlat

A G csoport akkor és csak akkor izomorf $A \times B \times C$-vel, ha vannak benne ezekkel izomorf olyan A^*, B^*, C^* normálosztók,

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek, akkor a sík (additív csoportja) nem lesz $e \oplus f \oplus g$.

4.9.14. Gyakorlat

A G csoport akkor és csak akkor izomorf $A \times B \times C$-vel, ha vannak benne ezekkel izomorf olyan A^*, B^*, C^* normálosztók, hogy $G = A^*B^*C^*$, továbbá

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek, akkor a sík (additív csoportja) nem lesz $e \oplus f \oplus g$.

4.9.14. Gyakorlat

A G csoport akkor és csak akkor izomorf $A \times B \times C$-vel, ha vannak benne ezekkel izomorf olyan A^*, B^*, C^* normálosztók, hogy $G = A^*B^*C^*$, továbbá
$A^* \cap (B^*C^*) = \{1\}$,

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek, akkor a sík (additív csoportja) nem lesz $e \oplus f \oplus g$.

4.9.14. Gyakorlat

A G csoport akkor és csak akkor izomorf $A \times B \times C$-vel, ha vannak benne ezekkel izomorf olyan A^*, B^*, C^* normálosztók, hogy $G = A^*B^*C^*$, továbbá
$A^* \cap (B^*C^*) = \{1\}$, $B^* \cap (A^*C^*) = \{1\}$,

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek,
akkor a sík (additív csoportja) nem lesz $e \oplus f \oplus g$.

4.9.14. Gyakorlat

A G csoport akkor és csak akkor izomorf $A \times B \times C$-vel,
ha vannak benne ezekkel izomorf olyan A^*, B^*, C^*
normálosztók, hogy $G = A^*B^*C^*$, továbbá
$A^* \cap (B^*C^*) = \{1\}$, $B^* \cap (A^*C^*) = \{1\}$, $C^* \cap (A^*B^*) = \{1\}$. $\square$

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek, akkor a sík (additív csoportja) nem lesz $e \oplus f \oplus g$.

4.9.14. Gyakorlat

A G csoport akkor és csak akkor izomorf $A \times B \times C$-vel, ha vannak benne ezekkel izomorf olyan A^*, B^*, C^* normálosztók, hogy $G = A^*B^*C^*$, továbbá
$A^* \cap (B^*C^*) = \{1\}$, $B^* \cap (A^*C^*) = \{1\}$, $C^* \cap (A^*B^*) = \{1\}$. □

Véges sok tényezőre:

Több tényezős direkt szorzat

Lineáris algebrában ugyanez a feltétel szerepelt:
$V = U \oplus W$ ha $U \cap W = \{0\}$ és $U + W = V$.
Ebből az additív csoportra kapunk direkt felbontásokat.
Például a sík két koordinátatengely direkt összege.

Ha e, f, g origón átmenő, páronként különböző egyenesek,
akkor a sík (additív csoportja) nem lesz $e \oplus f \oplus g$.

4.9.14. Gyakorlat

A G csoport akkor és csak akkor izomorf $A \times B \times C$-vel,
ha vannak benne ezekkel izomorf olyan A^*, B^*, C^*
normálosztók, hogy $G = A^* B^* C^*$, továbbá
$A^* \cap (B^* C^*) = \{1\}, \;\; B^* \cap (A^* C^*) = \{1\}, \;\; C^* \cap (A^* B^*) = \{1\}.$ □

Véges sok tényezőre: mindegyik „diszjunkt” a többiek szorzatától.

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$.

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^{\times}$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$,

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$,

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B$

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C$

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C$

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^{\times}$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.
Abel-csoportban minden részcsoport normálosztó.

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.
Abel-csoportban minden részcsoport normálosztó.
Ha A, B részcsoportok, akkor $|AB| = |A||B|/|A \cap B|$
(4.4.31. Gyakorlat).

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.
Abel-csoportban minden részcsoport normálosztó.
Ha A, B részcsoportok, akkor $|AB| = |A||B|/|A \cap B|$
(4.4.31. Gyakorlat). Így ha $A \cap B = \{1\}$, akkor $|AB| = |A||B|$.

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.
Abel-csoportban minden részcsoport normálosztó.
Ha A, B részcsoportok, akkor $|AB| = |A||B|/|A \cap B|$
(4.4.31. Gyakorlat). Így ha $A \cap B = \{1\}$, akkor $|AB| = |A||B|$.

4.9.25. Gyakorlat

Legyen $G = D_6$ (a 12 elemű diédercsoport).

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.
Abel-csoportban minden részcsoport normálosztó.
Ha A, B részcsoportok, akkor $|AB| = |A||B|/|A \cap B|$
(4.4.31. Gyakorlat). Így ha $A \cap B = \{1\}$, akkor $|AB| = |A||B|$.

4.9.25. Gyakorlat

Legyen $G = D_6$ (a 12 elemű diédercsoport).
Ha $A = \{1, f^3\}$

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.
Abel-csoportban minden részcsoport normálosztó.
Ha A, B részcsoportok, akkor $|AB| = |A||B|/|A \cap B|$
(4.4.31. Gyakorlat). Így ha $A \cap B = \{1\}$, akkor $|AB| = |A||B|$.

4.9.25. Gyakorlat

Legyen $G = D_6$ (a 12 elemű diédercsoport).
Ha $A = \{1, f^3\}$ és $B = \{1, f^2, f^4, t, tf^2, tf^4\}$,

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.
Abel-csoportban minden részcsoport normálosztó.
Ha A, B részcsoportok, akkor $|AB| = |A||B|/|A \cap B|$
(4.4.31. Gyakorlat). Így ha $A \cap B = \{1\}$, akkor $|AB| = |A||B|$.

4.9.25. Gyakorlat

Legyen $G = D_6$ (a 12 elemű diédercsoport).
Ha $A = \{1, f^3\}$ és $B = \{1, f^2, f^4, t, tf^2, tf^4\}$,
akkor $G = D_6 \cong A \times B$

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.
Abel-csoportban minden részcsoport normálosztó.
Ha A, B részcsoportok, akkor $|AB| = |A||B|/|A \cap B|$
(4.4.31. Gyakorlat). Így ha $A \cap B = \{1\}$, akkor $|AB| = |A||B|$.

4.9.25. Gyakorlat

Legyen $G = D_6$ (a 12 elemű diédercsoport).
Ha $A = \{1, f^3\}$ és $B = \{1, f^2, f^4, t, tf^2, tf^4\}$,
akkor $G = D_6 \cong A \times B \cong \mathbb{Z}_2^+ \times D_3$.

Példa direkt felbontásra

4.9.3. Gyakorlat

Legyen $G = \mathbb{Z}_8^\times$. Minden elem másodrendű, kivéve 1.
Ha $A = \{1, 3\}$, $B = \{1, 5\}$, $C = \{1, 7\}$,
akkor $G \cong A \times B \cong A \times C \cong B \times C \cong \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.
Abel-csoportban minden részcsoport normálosztó.
Ha A, B részcsoportok, akkor $|AB| = |A||B|/|A \cap B|$
(4.4.31. Gyakorlat). Így ha $A \cap B = \{1\}$, akkor $|AB| = |A||B|$.

4.9.25. Gyakorlat

Legyen $G = D_6$ (a 12 elemű diédercsoport).
Ha $A = \{1, f^3\}$ és $B = \{1, f^2, f^4, t, tf^2, tf^4\}$,
akkor $G = D_6 \cong A \times B \cong \mathbb{Z}_2^+ \times D_3$.
A B a szabályos hatszögbe írt szabályos háromszöget (mindegy melyiket) megőrző szimmetriákból álló részcsoport.

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

4.4.23. Tétel

Ha p prím, akkor minden p rendű csoport izomorf $\mathbb{Z}_p^+$-szal.

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

4.4.23. Tétel

Ha p prím, akkor minden p rendű csoport izomorf $\mathbb{Z}_p^+$-szal.

Vagyis izomorfia erejéig csak egy darab p elemű csoport van.

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

4.4.23. Tétel

Ha p prím, akkor minden p rendű csoport izomorf $\mathbb{Z}_p^+$-szal.

Vagyis izomorfia erejéig csak egy darab p elemű csoport van.

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

4.4.23. Tétel

Ha p prím, akkor minden p rendű csoport izomorf $\mathbb{Z}_p^+$-szal.

Vagyis izomorfia erejéig csak egy darab p elemű csoport van.

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_8^\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

4.4.23. Tétel

Ha p prím, akkor minden p rendű csoport izomorf $\mathbb{Z}_p^+$-szal.

Vagyis izomorfia erejéig csak egy darab p elemű csoport van.

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_8^\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

4.4.23. Tétel

Ha p prím, akkor minden p rendű csoport izomorf $\mathbb{Z}_p^+$-szal.

Vagyis izomorfia erejéig csak egy darab p elemű csoport van.

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_8^\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4^+ \cong \mathbb{Z}_5^\times$,

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

4.4.23. Tétel

Ha p prím, akkor minden p rendű csoport izomorf $\mathbb{Z}_p^+$-szal.

Vagyis izomorfia erejéig csak egy darab p elemű csoport van.

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_8^\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4^+ \cong \mathbb{Z}_5^\times$, de nem izomorfak $\mathbb{Z}_8^\times$-cal,

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

4.4.23. Tétel

Ha p prím, akkor minden p rendű csoport izomorf $\mathbb{Z}_p^+$-szal.

Vagyis izomorfia erejéig csak egy darab p elemű csoport van.

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_8^\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4^+ \cong \mathbb{Z}_5^\times$, de nem izomorfak $\mathbb{Z}_8^\times$-cal, mert abban nincs negyedrendű elem,

Ismétlés

Minden kételemű csoport izomorf $\mathbb{Z}_2^+$-szal.

4.4.23. Tétel

Ha p prím, akkor minden p rendű csoport izomorf $\mathbb{Z}_p^+$-szal.

Vagyis izomorfia erejéig csak egy darab p elemű csoport van.

$\mathbb{Z}_5^\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_8^\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4^+ \cong \mathbb{Z}_5^\times$, de nem izomorfak $\mathbb{Z}_8^\times$-cal, mert abban nincs negyedrendű elem, vagyis nem ciklikus.

Négyelemű csoportok

A Klein-csoport:

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Példák Klein-csoportra:

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja,

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$,

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$,

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,
$\{1, f^2, t, tf^2\} \leq D_4$,

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,
$\{1, f^2, t, tf^2\} \leq D_4$, $\{id, (12)(34), (13)(24), (14)(23)\} \leq A_4$.

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

ciklikus:

	1	g	g^2	g^3
1	1	g	g^2	g^3
g	g	g^2	g^3	1
g^2	g^2	g^3	1	g
g^3	g^3	1	g	g^2

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,
$\{1, f^2, t, tf^2\} \leq D_4$, $\{id, (12)(34), (13)(24), (14)(23)\} \leq A_4$.

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

ciklikus:

	1	g	g^2	g^3
1	1	g	g^2	g^3
g	g	g^2	g^3	1
g^2	g^2	g^3	1	g
g^3	g^3	1	g	g^2

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,
$\{1, f^2, t, tf^2\} \leq D_4$, $\{id, (12)(34), (13)(24), (14)(23)\} \leq A_4$.

Példák négyelemű ciklikus csoportra:

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

ciklikus:

	1	g	g^2	g^3
1	1	g	g^2	g^3
g	g	g^2	g^3	1
g^2	g^2	g^3	1	g
g^3	g^3	1	g	g^2

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,
$\{1, f^2, t, tf^2\} \leq D_4$, $\{id, (12)(34), (13)(24), (14)(23)\} \leq A_4$.

Példák négyelemű ciklikus csoportra:

$\mathbb{Z}_4^+$,

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

ciklikus:

	1	g	g^2	g^3
1	1	g	g^2	g^3
g	g	g^2	g^3	1
g^2	g^2	g^3	1	g
g^3	g^3	1	g	g^2

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,
$\{1, f^2, t, tf^2\} \leq D_4$, $\{id, (12)(34), (13)(24), (14)(23)\} \leq A_4$.

Példák négyelemű ciklikus csoportra:

$\mathbb{Z}_4^+$, $\mathbb{Z}_5^\times$,

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

ciklikus:

	1	g	g^2	g^3
1	1	g	g^2	g^3
g	g	g^2	g^3	1
g^2	g^2	g^3	1	g
g^3	g^3	1	g	g^2

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,
$\{1, f^2, t, tf^2\} \leq D_4$, $\{id, (12)(34), (13)(24), (14)(23)\} \leq A_4$.

Példák négyelemű ciklikus csoportra:

$\mathbb{Z}_4^+$, $\mathbb{Z}_5^\times$, $\{1, f, f^2, f^3\} \leq D_4$,

Négyelemű csoportok

A Klein-csoport: minden elem négyzete az egységelem;
Bármely két egységtől különböző elem szorzata a harmadik.

Klein:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

ciklikus:

	1	g	g^2	g^3
1	1	g	g^2	g^3
g	g	g^2	g^3	1
g^2	g^2	g^3	1	g
g^3	g^3	1	g	g^2

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,
$\{1, f^2, t, tf^2\} \leq D_4$, $\{id, (12)(34), (13)(24), (14)(23)\} \leq A_4$.

Példák négyelemű ciklikus csoportra:

$\mathbb{Z}_4^+$, $\mathbb{Z}_5^\times$, $\{1, f, f^2, f^3\} \leq D_4$, $\{id, (1234), (13)(24), (1432)\} \leq S_4$.

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal,

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf,

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$.

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű,

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs,

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus. Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$.

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus. Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2,

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab = ?$

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus. Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1,

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies$

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies \quad 1b = abb$

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies b = 1b = abb$

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies b = 1b = abb = a$.

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies b = 1b = abb = a$.
Nem a,

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies b = 1b = abb = a$.
Nem a, mert $ab = a$-t a-val egyszerűsítve

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies b = 1b = abb = a$.
Nem a, mert $ab = a$-t a-val egyszerűsítve $b = 1$ lenne.

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies b = 1b = abb = a$.
Nem a, mert $ab = a$-t a-val egyszerűsítve $b = 1$ lenne.
Hasonlóképpen ab nem lehet b,

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies b = 1b = abb = a$.
Nem a, mert $ab = a$-t a-val egyszerűsítve $b = 1$ lenne.
Hasonlóképpen ab nem lehet b, tehát $ab = c$.

A négyelemű csoportok osztályozása

4.5.18. Tétel

Minden négyelemű csoport a négyelemű ciklikus csoporttal, vagy a Klein-csoporttal izomorf, attól függően, hogy van-e benne negyedrendű elem, vagy nincs.

Bizonyítás

Legyen $|G| = 4$. Ha van negyedrendű elem, akkor az általa generált részcsoport négyelemű, tehát G ciklikus.
Tegyük föl, hogy nincs, legyen $G = \{1, a, b, c\}$. Ekkor a, b, c rendje Lagrange tétele miatt 2, azaz $a^2 = b^2 = c^2 = 1$.
$ab =?$ Nem 1, mert $ab = 1 \implies b = 1b = abb = a$.
Nem a, mert $ab = a$-t a-val egyszerűsítve $b = 1$ lenne.
Hasonlóképpen ab nem lehet b, tehát $ab = c$.
Ugyanígy: a, b, c közül bármely kettő szorzata a harmadik. $\square$

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

A bizonyítás konjugált elemosztályokkal történik, nem kell tudni.

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

A bizonyítás konjugált elemosztályokkal történik, nem kell tudni.

Következmény

Ha p prím, akkor izomorfia erejéig két p^2 rendű csoport van:

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

A bizonyítás konjugált elemosztályokkal történik, nem kell tudni.

Következmény

Ha p prím, akkor izomorfia erejéig két p^2 rendű csoport van:
$\mathbb{Z}_{p^2}^+$

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

A bizonyítás konjugált elemosztályokkal történik, nem kell tudni.

Következmény

Ha p prím, akkor izomorfia erejéig két p^2 rendű csoport van: $\mathbb{Z}_{p^2}^+$ és $\mathbb{Z}_p^+ \times \mathbb{Z}_p^+$.

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

A bizonyítás konjugált elemosztályokkal történik, nem kell tudni.

Következmény

Ha p prím, akkor izomorfia erejéig két p^2 rendű csoport van: $\mathbb{Z}^+_{p^2}$ és $\mathbb{Z}^+_p \times \mathbb{Z}^+_p$.

Ezek nem izomorfak a véges Abel-csoportok alaptételének egyértelműségi állítása miatt,

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

A bizonyítás konjugált elemosztályokkal történik, nem kell tudni.

Következmény

Ha p prím, akkor izomorfia erejéig két p^2 rendű csoport van: $\mathbb{Z}_{p^2}^+$ és $\mathbb{Z}_p^+ \times \mathbb{Z}_p^+$.

Ezek nem izomorfak a véges Abel-csoportok alaptételének egyértelműségi állítása miatt, vagy mert $(\mathbb{Z}_p^+)^2$ nem ciklikus.

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

A bizonyítás konjugált elemosztályokkal történik, nem kell tudni.

Következmény

Ha p prím, akkor izomorfia erejéig két p^2 rendű csoport van: $\mathbb{Z}_{p^2}^+$ és $\mathbb{Z}_p^+ \times \mathbb{Z}_p^+$.

Ezek nem izomorfak a véges Abel-csoportok alaptételének egyértelműségi állítása miatt, vagy mert $(\mathbb{Z}_p^+)^2$ nem ciklikus.

Tehát izomorfia erejéig rendre két $4, 9, 25$ rendű csoport van.

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

A bizonyítás konjugált elemosztályokkal történik, nem kell tudni.

Következmény

Ha p prím, akkor izomorfia erejéig két p^2 rendű csoport van: $\mathbb{Z}_{p^2}^+$ és $\mathbb{Z}_p^+ \times \mathbb{Z}_p^+$.

Ezek nem izomorfak a véges Abel-csoportok alaptételének egyértelműségi állítása miatt, vagy mert $(\mathbb{Z}_p^+)^2$ nem ciklikus.

Tehát izomorfia erejéig rendre két $4, 9, 25$ rendű csoport van. Izomorfia erejéig egy-egy $1, 2, 3, 5, 7, 11, 13$ rendű csoport van.

Prímnégyzet elemszámú csoportok

4.11.3. Következmény

Minden prímnégyzet rendű csoport kommutatív.

A bizonyítás konjugált elemosztályokkal történik, nem kell tudni.

Következmény

Ha p prím, akkor izomorfia erejéig két p^2 rendű csoport van: $\mathbb{Z}_{p^2}^+$ és $\mathbb{Z}_p^+ \times \mathbb{Z}_p^+$.

Ezek nem izomorfak a véges Abel-csoportok alaptételének egyértelműségi állítása miatt, vagy mert $(\mathbb{Z}_p^+)^2$ nem ciklikus.

Tehát izomorfia erejéig rendre két $4, 9, 25$ rendű csoport van.
Izomorfia erejéig egy-egy $1, 2, 3, 5, 7, 11, 13$ rendű csoport van.

Kimaradt: 6, 8, 10, 12.

Hatodrendű csoportok

4.8.37. Gyakorlat (NB)

Legyen p páratlan prímszám.

Hatodrendű csoportok

4.8.37. Gyakorlat (NB)

Legyen p páratlan prímszám. Ekkor egy $2p$ rendű csoport vagy ciklikus,

Hatodrendű csoportok

4.8.37. Gyakorlat (NB)

Legyen p páratlan prímszám. Ekkor egy $2p$ rendű csoport vagy ciklikus, vagy a D_p diédercsoporttal izomorf.

Hatodrendű csoportok

4.8.37. Gyakorlat (NB)

Legyen p páratlan prímszám. Ekkor egy $2p$ rendű csoport vagy ciklikus, vagy a D_p diédercsoporttal izomorf.

Nem izomorfak, mert csak az egyik kommutatív.

Hatodrendű csoportok

4.8.37. Gyakorlat (NB)

Legyen p páratlan prímszám. Ekkor egy $2p$ rendű csoport vagy ciklikus, vagy a D_p diédercsoporttal izomorf.

Nem izomorfak, mert csak az egyik kommutatív.

Következmény

Tehát hatodrendű és tizedrendű csoportból is kettő van.

Hatodrendű csoportok

4.8.37. Gyakorlat (NB)

Legyen p páratlan prímszám. Ekkor egy $2p$ rendű csoport vagy ciklikus, vagy a D_p diédercsoporttal izomorf.

Nem izomorfak, mert csak az egyik kommutatív.

Következmény

Tehát hatodrendű és tizedrendű csoportból is kettő van.

4.5.16. Gyakorlat: $S_3 \cong D_3$.

Hatodrendű csoportok

4.8.37. Gyakorlat (NB)

Legyen p páratlan prímszám. Ekkor egy $2p$ rendű csoport vagy ciklikus, vagy a D_p diédercsoporttal izomorf.

Nem izomorfak, mert csak az egyik kommutatív.

Következmény

Tehát hatodrendű és tizedrendű csoportból is kettő van.

4.5.16. Gyakorlat: $S_3 \cong D_3$.

Bizonyítás

Mindkettő egy háromelemű halmaz összes permutációiból áll.

Hatodrendű csoportok

4.8.37. Gyakorlat (NB)

Legyen p páratlan prímszám. Ekkor egy $2p$ rendű csoport vagy ciklikus, vagy a D_p diédercsoporttal izomorf.

Nem izomorfak, mert csak az egyik kommutatív.

Következmény

Tehát hatodrendű és tizedrendű csoportból is kettő van.

4.5.16. Gyakorlat: $S_3 \cong D_3$.

Bizonyítás

Mindkettő egy háromelemű halmaz összes permutációiból áll.
A D_3 esetében ezek a szabályos háromszög csúcsai.

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.

Nemkommutatívak: a D_4 diédercsoport

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.

Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.

Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.

Kommutatívak: $\mathbb{Z}_8^+$,

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$,

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.

Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.

Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.

Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.

Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val,

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val, mert D_4-ben öt darab, másodrendű elem van.

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val, mert D_4-ben öt darab, Q-ban pedig csak egy darab másodrendű elem van.

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val, mert D_4-ben öt darab, Q-ban pedig csak egy darab másodrendű elem van.
A három kommutatív csoport is páronként nemizomorf:

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val, mert D_4-ben öt darab,
Q-ban pedig csak egy darab másodrendű elem van.
A három kommutatív csoport is páronként nemizomorf:
a másodrendű elemek száma rendre 1,

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val, mert D_4-ben öt darab,
Q-ban pedig csak egy darab másodrendű elem van.
A három kommutatív csoport is páronként nemizomorf:
a másodrendű elemek száma rendre 1, 3,

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val, mert D_4-ben öt darab,
Q-ban pedig csak egy darab másodrendű elem van.
A három kommutatív csoport is páronként nemizomorf:
a másodrendű elemek száma rendre 1, 3, 7.

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val, mert D_4-ben öt darab,
Q-ban pedig csak egy darab másodrendű elem van.
A három kommutatív csoport is páronként nemizomorf:
a másodrendű elemek száma rendre 1, 3, 7.

4.11. szakasz (NB)

Minden p prímre két nemkommutatív
p^3 rendű csoport van.

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val, mert D_4-ben öt darab,
Q-ban pedig csak egy darab másodrendű elem van.
A három kommutatív csoport is páronként nemizomorf:
a másodrendű elemek száma rendre 1, 3, 7.

4.11. szakasz (NB)

Minden p prímre két nemkommutatív
és három kommutatív p^3 rendű csoport van.

Nyolcadrendű csoportok

4.11.10. Feladat (NB)

Nyolcadrendű csoport ötféle létezik.
Nemkommutatívak: a D_4 diédercsoport és a Q kvaterniócsoport.
Kommutatívak: $\mathbb{Z}_8^+$, $\mathbb{Z}_4^+ \times \mathbb{Z}_2^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+$.

D_4 nem izomorf Q-val, mert D_4-ben öt darab, Q-ban pedig csak egy darab másodrendű elem van.
A három kommutatív csoport is páronként nemizomorf: a másodrendű elemek száma rendre 1, 3, 7.

4.11. szakasz (NB)

Minden p prímre két nemkommutatív és három kommutatív p^3 rendű csoport van.

A kis (legfeljebb 30 elemű) csoportok táblázata: jegyzet, 682. oldal.

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll.

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$,

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív,

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix,

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$.

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$. Mivel $EN = NE$, ezért
$(E + N)^p = E^p + pE^{p-1}N + [(p-1)/2]pE^{p-2}N^2$

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$. Mivel $EN = NE$, ezért $(E + N)^p = E^p + pE^{p-1}N + [(p-1)/2]pE^{p-2}N^2$ (alkalmazható a binomiális tétel,

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$. Mivel $EN = NE$, ezért $(E + N)^p = E^p + pE^{p-1}N + [(p-1)/2]pE^{p-2}N^2$ (alkalmazható a binomiális tétel, az összeg többi tagja nulla.)

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$. Mivel $EN = NE$, ezért $(E + N)^p = E^p + pE^{p-1}N + [(p-1)/2]pE^{p-2}N^2$ (alkalmazható a binomiális tétel, az összeg többi tagja nulla.) A $\mathbb{Z}_p$ test fölött $pN = 0$.

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$. Mivel $EN = NE$, ezért $(E + N)^p = E^p + pE^{p-1}N + [(p-1)/2]pE^{p-2}N^2$ (alkalmazható a binomiális tétel, az összeg többi tagja nulla.) A $\mathbb{Z}_p$ test fölött $pN = 0$. Mivel p páratlan, $(p-1)/2$ egész,

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$. Mivel $EN = NE$, ezért $(E + N)^p = E^p + pE^{p-1}N + [(p-1)/2]pE^{p-2}N^2$ (alkalmazható a binomiális tétel, az összeg többi tagja nulla.) A $\mathbb{Z}_p$ test fölött $pN = 0$. Mivel p páratlan, $(p-1)/2$ egész, és ezért az összeg harmadik tagja is nulla,

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$. Mivel $EN = NE$, ezért $(E + N)^p = E^p + pE^{p-1}N + [(p-1)/2]pE^{p-2}N^2$ (alkalmazható a binomiális tétel, az összeg többi tagja nulla.) A $\mathbb{Z}_p$ test fölött $pN = 0$. Mivel p páratlan, $(p-1)/2$ egész, és ezért az összeg harmadik tagja is nulla, azaz $(E + N)^p = E$.

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$. Mivel $EN = NE$, ezért $(E + N)^p = E^p + pE^{p-1}N + [(p-1)/2]pE^{p-2}N^2$ (alkalmazható a binomiális tétel, az összeg többi tagja nulla.) A $\mathbb{Z}_p$ test fölött $pN = 0$. Mivel p páratlan, $(p-1)/2$ egész, és ezért az összeg harmadik tagja is nulla, azaz $(E + N)^p = E$. A G rendjének leolvasása és a nemkommutativitás bizonyítása HF. $\square$

p exponensű, nemkommutatív csoport

4.11.12. Gyakorlat

Legyen p páratlan prím, és álljon $G \leq \mathrm{GL}(3, \mathbb{Z}_p)$ azon mátrixokból, melyek főátlójában végig 1, alatta csupa nulla áll. Ekkor $|G| = p^3$, G nem kommutatív, és minden $\neq 1$ elemének rendje p.

Bizonyítás

G elemei $E + N$ alakúak, ahol E az egységmátrix, N szigorú felső háromszögmátrix, és így $N^3 = 0$. Mivel $EN = NE$, ezért $(E + N)^p = E^p + pE^{p-1}N + [(p-1)/2]pE^{p-2}N^2$ (alkalmazható a binomiális tétel, az összeg többi tagja nulla.) A $\mathbb{Z}_p$ test fölött $pN = 0$. Mivel p páratlan, $(p-1)/2$ egész, és ezért az összeg harmadik tagja is nulla, azaz $(E + N)^p = E$. A G rendjének leolvasása és a nemkommutativitás bizonyítása HF. $\square$

G-ben és $(\mathbb{Z}_p^+)^3$-ben ugyanazok az elemrendek, de nem izomorfak.

A kocka szimmetriacsoportja

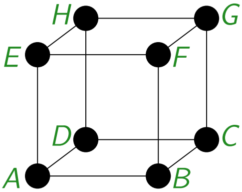
4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.

A kocka szimmetriacsoportja

4.9.32. Feladat

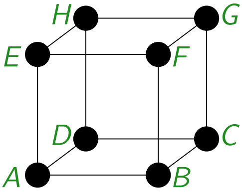
A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.

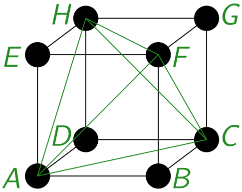


$ACFH$ szabályos tetraéder.

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.

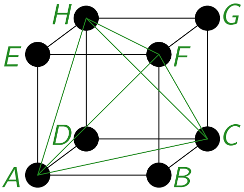


$ACFH$ szabályos tetraéder.

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.

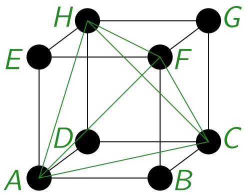


$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



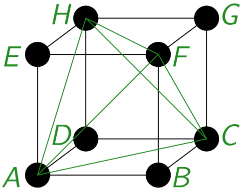
$ACFH$ szabályos tetraéder. $BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



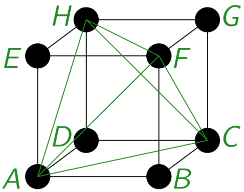
$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.
Legyen K az $ACFH$ stabilizátora.

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



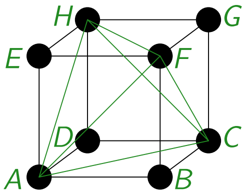
$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.
Legyen K az $ACFH$ stabilizátora. A pálya-stabilizátor-tétel miatt a K részcsoport indexe 2,

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



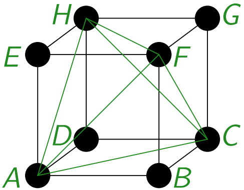
$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.
Legyen K az $ACFH$ stabilizátora. A pálya-stabilizátor-tétel miatt a K részcsoport indexe 2, és így K normálosztó.

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



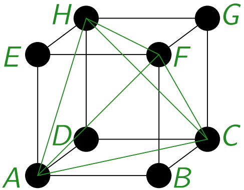
$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.
Legyen K az $ACFH$ stabilizátora. A pálya-stabilizátor-tétel miatt a K részcsoport indexe 2, és így K normálosztó.
Továbbá $K \cong S_4$,

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



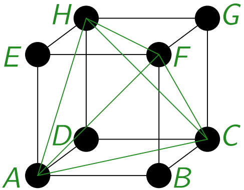
$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.
Legyen K az $ACFH$ stabilizátora. A pálya-stabilizátor-tétel miatt a K részcsoport indexe 2, és így K normálosztó.
Továbbá $K \cong S_4$, hiszen 24 elemű,

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



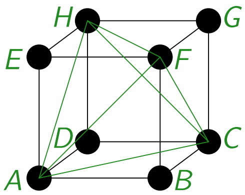
$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.
Legyen K az $ACFH$ stabilizátora. A pálya-stabilizátor-tétel miatt a K részcsoport indexe 2, és így K normálosztó.
Továbbá $K \cong S_4$, hiszen 24 elemű, és része $S_{\{A,C,F,H\}}$-nak.

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



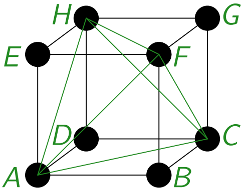
$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.
Legyen K az $ACFH$ stabilizátora. A pálya-stabilizátor-tétel miatt a K részcsoport indexe 2, és így K normálosztó.
Továbbá $K \cong S_4$, hiszen 24 elemű, és része $S_{\{A,C,F,H\}}$-nak.
Legyen $L = \{id, r\}$, ahol r a középpontos tükrözés.

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



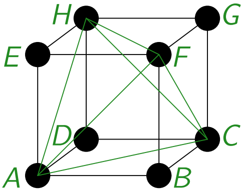
$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.
Legyen K az $ACFH$ stabilizátora. A pálya-stabilizátor-tétel miatt a K részcsoport indexe 2, és így K normálosztó.
Továbbá $K \cong S_4$, hiszen 24 elemű, és része $S_{\{A,C,F,H\}}$-nak.
Legyen $L = \{id, r\}$, ahol r a középpontos tükrözés.
L normálosztó, mert r minden transzformációval felcserélhető.

A kocka szimmetriacsoportja

4.9.32. Feladat

A kocka szimmetriacsoportja izomorf $S_4 \times \mathbb{Z}_2^+$-vel.



$ACFH$ szabályos tetraéder.
$BDEG$ szintén.

G tranzitívan hat a két tetraéderből álló halmazon.
Legyen K az $ACFH$ stabilizátora. A pálya-stabilizátor-tétel miatt a K részcsoport indexe 2, és így K normálosztó.
Továbbá $K \cong S_4$, hiszen 24 elemű, és része $S_{\{A,C,F,H\}}$-nak.
Legyen $L = \{id, r\}$, ahol r a középpontos tükrözés.
L normálosztó, mert r minden transzformációval felcserélhető.
Így $G \cong K \times L$.

Kommutatív egyszerű csoportok

4.8.2. Definíció

A G csoportot egyszerű csoportnak nevezzük,

Kommutatív egyszerű csoportok

4.8.2. Definíció

A G csoportot egyszerű csoportnak nevezzük, ha pontosan két normálosztója van:

Kommutatív egyszerű csoportok

4.8.2. Definíció

A G csoportot egyszerű csoportnak nevezzük, ha pontosan két normálosztója van: a triviálisak

Kommutatív egyszerű csoportok

4.8.2. Definíció

A G csoportot egyszerű csoportnak nevezzük, ha pontosan két normálosztója van: a triviálisak (vagyis $\{1\}$ és G).

Kommutatív egyszerű csoportok

4.8.2. Definíció

A G csoportot egyszerű csoportnak nevezzük, ha pontosan két normálosztója van: a triviálisak (vagyis $\{1\}$ és G). (Az egyelemű csoport nem egyszerű!)

Kommutatív egyszerű csoportok

4.8.2. Definíció

A G csoportot egyszerű csoportnak nevezzük, ha pontosan két normálosztója van: a triviálisak (vagyis $\{1\}$ és G). (Az egyelemű csoport nem egyszerű!)

4.8.3. Következmény

A kommutatív egyszerű csoportok pontosan a prímrendű ciklikus csoportok.

Kommutatív egyszerű csoportok

4.8.2. Definíció

A G csoportot egyszerű csoportnak nevezzük, ha pontosan két normálosztója van: a triviálisak (vagyis $\{1\}$ és G). (Az egyelemű csoport nem egyszerű!)

4.8.3. Következmény

A kommutatív egyszerű csoportok pontosan a prímrendű ciklikus csoportok.

Bizonyítás

Egy Abel-csoportban minden részcsoport nyilván normálosztó.

Kommutatív egyszerű csoportok

4.8.2. Definíció

A G csoportot egyszerű csoportnak nevezzük, ha pontosan két normálosztója van: a triviálisak (vagyis $\{1\}$ és G). (Az egyelemű csoport nem egyszerű!)

4.8.3. Következmény

A kommutatív egyszerű csoportok pontosan a prímrendű ciklikus csoportok.

Bizonyítás

Egy Abel-csoportban minden részcsoport nyilván normálosztó. Tehát a kommutatív egyszerű csoportok azok, amelyeknek pontosan két részcsoportja van.

Kommutatív egyszerű csoportok

4.8.2. Definíció

A G csoportot egyszerű csoportnak nevezzük, ha pontosan két normálosztója van: a triviálisak (vagyis $\{1\}$ és G). (Az egyelemű csoport nem egyszerű!)

4.8.3. Következmény

A kommutatív egyszerű csoportok pontosan a prímrendű ciklikus csoportok.

Bizonyítás

Egy Abel-csoportban minden részcsoport nyilván normálosztó. Tehát a kommutatív egyszerű csoportok azok, amelyeknek pontosan két részcsoportja van. Láttuk, hogy ezek pont a prímrendű ciklikus csoportok. $\square$

Két fontos példa

4.12.30. Tétel (NB)

Az A_n alternáló csoport egyszerű, ha $n \geq 5$.

Két fontos példa

4.12.30. Tétel (NB)

Az A_n alternáló csoport egyszerű, ha $n \geq 5$.

Következmény: A legalább ötödfokú általános egyenletekre nincs megoldóképlet

Két fontos példa

4.12.30. Tétel (NB)

Az A_n alternáló csoport egyszerű, ha $n \geq 5$.

Következmény: A legalább ötödfokú általános egyenletekre nincs megoldóképlet (négy alapművelettel és gyökvonással).

Két fontos példa

4.12.30. Tétel (NB)

Az A_n alternáló csoport egyszerű, ha $n \geq 5$.

Következmény: A legalább ötödfokú általános egyenletekre nincs megoldóképlet (négy alapművelettel és gyökvonással).

4.12.36. Gyakorlat (NB)

Ha $n \geq 5$, akkor S_n egyetlen nemtriviális normálosztója A_n.

Két fontos példa

4.12.30. Tétel (NB)

Az A_n alternáló csoport egyszerű, ha $n \geq 5$.

Következmény: A legalább ötödfokú általános egyenletekre nincs megoldóképlet (négy alapművelettel és gyökvonással).

4.12.36. Gyakorlat (NB)

Ha $n \geq 5$, akkor S_n egyetlen nemtriviális normálosztója A_n.

4.8.42. Feladat (NB)

A gömb mozgáscsoportja, azaz $\mathrm{SO}(3)$ egyszerű csoport.

Két fontos példa

4.12.30. Tétel (NB)

Az A_n alternáló csoport egyszerű, ha $n \geq 5$.

Következmény: A legalább ötödfokú általános egyenletekre nincs megoldóképlet (négy alapművelettel és gyökvonással).

4.12.36. Gyakorlat (NB)

Ha $n \geq 5$, akkor S_n egyetlen nemtriviális normálosztója A_n.

4.8.42. Feladat (NB)

A gömb mozgáscsoportja, azaz $\mathrm{SO}(3)$ egyszerű csoport.

4.9.13. Gyakorlat (NB)

A gömb szimmetriacsoportja, $\mathrm{O}(3) \cong \mathrm{SO}(3) \times \mathbb{Z}_2^+$.

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból:

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport,

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Az összerakás nem egyértelmű!

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$,

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk'' egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
$G = S_3$,

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk'' egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
$G = S_3$, $N = A_3 \cong \mathbb{Z}_3^+$

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
$G = S_3$, $N = A_3 \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
$G = S_3$, $N = A_3 \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
Tehát ugyanazokat az egyszerűeket kapjuk

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
$G = S_3$, $N = A_3 \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
Tehát ugyanazokat az egyszerűeket kapjuk ($\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$),

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk” egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
$G = S_3$, $N = A_3 \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
Tehát ugyanazokat az egyszerűeket kapjuk ($\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$), mégis $\mathbb{Z}_6^+$ és S_3 nem izomorfak.

Csoportok bővítése

Ha N normálosztó G-ben, akkor G-t megpróbálhatjuk összerakni N-ből és a G/N faktorcsoportból: bővítés.
N és G/N már kisebb csoport, így egyszerűbb szerkezetű.
Addig folytathatjuk, amíg egyszerű csoporthoz nem jutunk.
Így minden csoportot „szétbonthatunk" egyszerű csoportokra.

Az összerakás nem egyértelmű!

Példa

$G = \mathbb{Z}_6^+$, $N = \{0, 2, 4\} \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
$G = S_3$, $N = A_3 \cong \mathbb{Z}_3^+$ és $G/N \cong \mathbb{Z}_2^+$.
Tehát ugyanazokat az egyszerűeket kapjuk ($\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$), mégis $\mathbb{Z}_6^+$ és S_3 nem izomorfak.

Ennek ellenére a „G-be bezárt egyszerű csoportok" listája fontos információ minden csoportról.

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható,

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3$

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$,

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \triangleleft A_3 \triangleleft S_3$, a faktorok $\mathbb{Z}_3^+$

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \triangleleft A_3 \triangleleft S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \triangleleft A_3 \triangleleft S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \triangleleft \{id, (12)(34)\}$

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \triangleleft A_3 \triangleleft S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \triangleleft \{id, (12)(34)\} \triangleleft \{id, (12)(34), (13)(24), (14)(23)\}$

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4$

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
A faktorok rendre $\mathbb{Z}_2^+$,

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$,

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$,

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \triangleleft A_3 \triangleleft S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \triangleleft \{id, (12)(34)\} \triangleleft \{id, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4 \triangleleft S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$, $\mathbb{Z}_2^+$.

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \triangleleft A_3 \triangleleft S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \triangleleft \{id, (12)(34)\} \triangleleft \{id, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4 \triangleleft S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$, $\mathbb{Z}_2^+$.
Vigyázat! $\{id, (12)(34)\}$ nem normálosztó S_4-ben!

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$, $\mathbb{Z}_2^+$.
Vigyázat! $\{id, (12)(34)\}$ nem normálosztó S_4-ben!

$id \lhd A_5 \lhd S_5$,

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$, $\mathbb{Z}_2^+$.
Vigyázat! $\{id, (12)(34)\}$ nem normálosztó S_4-ben!

$id \lhd A_5 \lhd S_5$, és itt A_5 egyszerű,

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$, $\mathbb{Z}_2^+$.
Vigyázat! $\{id, (12)(34)\}$ nem normálosztó S_4-ben!

$id \lhd A_5 \lhd S_5$, és itt A_5 egyszerű, de nem prímrendű.

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$, $\mathbb{Z}_2^+$.
Vigyázat! $\{id, (12)(34)\}$ nem normálosztó S_4-ben!

$id \lhd A_5 \lhd S_5$, és itt A_5 egyszerű, de nem prímrendű.

A G-be „bezárt” egyszerű csoportok listája egyértelmű

Feloldható csoportok

Meseszerű definíció (precízen lásd 4.13.5. Definíció)

Feloldható: bővítéssel összerakható prímrendű ciklikusokból.

4.8.15. Állítás: S_3 és S_4 feloldható, de S_5 nem.

$id \lhd A_3 \lhd S_3$, a faktorok $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$.
Ezért van a Cardano-képletben köbgyök és négyzetgyök!!

$\{id\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
A faktorok rendre $\mathbb{Z}_2^+$, $\mathbb{Z}_2^+$, $\mathbb{Z}_3^+$, $\mathbb{Z}_2^+$.
Vigyázat! $\{id, (12)(34)\}$ nem normálosztó S_4-ben!

$id \lhd A_5 \lhd S_5$, és itt A_5 egyszerű, de nem prímrendű.

A G-be „bezárt" egyszerű csoportok listája egyértelmű (mindegy, hogyan bontjuk le): Jordan–Hölder-tétel (4.13.3).

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta
a szimmetriacsoportját.

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta
a szimmetriacsoportját. Belátta, hogy ez a csoport
pontosan akkor feloldható,

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta
a szimmetriacsoportját. Belátta, hogy ez a csoport
pontosan akkor feloldható, ha az egyenlet gyökeit fel lehet írni
a négy alapművelet és gyökvonás segítségével.

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta a szimmetriacsoportját. Belátta, hogy ez a csoport pontosan akkor feloldható, ha az egyenlet gyökeit fel lehet írni a négy alapművelet és gyökvonás segítségével.

Lásd jegyzet, 6.9. szakasz.

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta
a szimmetriacsoportját. Belátta, hogy ez a csoport
pontosan akkor feloldható, ha az egyenlet gyökeit fel lehet írni
a négy alapművelet és gyökvonás segítségével.

Lásd jegyzet, 6.9. szakasz.

6.6.15. Feladat (NB)

$x^5 - 4x + 2$ szimmetriacsoportja (Galois-csoportja) S_5.

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta
a szimmetriacsoportját. Belátta, hogy ez a csoport
pontosan akkor feloldható, ha az egyenlet gyökeit fel lehet írni
a négy alapművelet és gyökvonás segítségével.

Lásd jegyzet, 6.9. szakasz.

6.6.15. Feladat (NB)

$x^5 - 4x + 2$ szimmetriacsoportja (Galois-csoportja) S_5.
Ezért ennek a polinomnak a gyökei nem gyökkifejezések.

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta
a szimmetriacsoportját. Belátta, hogy ez a csoport
pontosan akkor feloldható, ha az egyenlet gyökeit fel lehet írni
a négy alapművelet és gyökvonás segítségével.

Lásd jegyzet, 6.9. szakasz.

6.6.15. Feladat (NB)

$x^5 - 4x + 2$ szimmetriacsoportja (Galois-csoportja) S_5.
Ezért ennek a polinomnak a gyökei nem gyökkifejezések.

$x^5 + 3x^4 - 4x^3 - 5x^2 + x + 1$ Galois-csoportja D_5,

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta
a szimmetriacsoportját. Belátta, hogy ez a csoport
pontosan akkor feloldható, ha az egyenlet gyökeit fel lehet írni
a négy alapművelet és gyökvonás segítségével.

Lásd jegyzet, 6.9. szakasz.

6.6.15. Feladat (NB)

$x^5 - 4x + 2$ szimmetriacsoportja (Galois-csoportja) S_5.
Ezért ennek a polinomnak a gyökei nem gyökkifejezések.

$x^5 + 3x^4 - 4x^3 - 5x^2 + x + 1$ Galois-csoportja D_5, feloldható.

Feloldhatóság és gyökképlet

Abel, 1824: az általános ötödfokú egyenletre nincs gyökképlet.
Galois, 1830 körül: minden egyenletnek definiálta a szimmetriacsoportját. Belátta, hogy ez a csoport pontosan akkor feloldható, ha az egyenlet gyökeit fel lehet írni a négy alapművelet és gyökvonás segítségével.

Lásd jegyzet, 6.9. szakasz.

6.6.15. Feladat (NB)

$x^5 - 4x + 2$ szimmetriacsoportja (Galois-csoportja) S_5.
Ezért ennek a polinomnak a gyökei nem gyökkifejezések.

$x^5 + 3x^4 - 4x^3 - 5x^2 + x + 1$ Galois-csoportja D_5, feloldható.
Ezért ennek a polinomnak a gyökei gyökkifejezések.

Prímhatványrendű csoportok

Cauchy, Sylow, 1840–80: prímhatványrendű csoportok.

Prímhatványrendű csoportok

Cauchy, Sylow, 1840–80: prímhatványrendű csoportok.

Lásd jegyzet, 4.11 szakasz.

Prímhatványrendű csoportok

Cauchy, Sylow, 1840–80: prímhatványrendű csoportok.

Lásd jegyzet, 4.11 szakasz.

4.11.5. Következmény (NB)

Ha egy prímhatványrendű csoport egyszerű, akkor az prímrendű ciklikus csoport.

Prímhatványrendű csoportok

Cauchy, Sylow, 1840–80: prímhatványrendű csoportok.

Lásd jegyzet, 4.11 szakasz.

4.11.5. Következmény (NB)

Ha egy prímhatványrendű csoport egyszerű, akkor az prímrendű ciklikus csoport.

4.13.10. Következmény

Minden prímhatványrendű csoport feloldható.

Prímhatványrendű csoportok

Cauchy, Sylow, 1840–80: prímhatványrendű csoportok.

Lásd jegyzet, 4.11 szakasz.

4.11.5. Következmény (NB)

Ha egy prímhatványrendű csoport egyszerű, akkor az prímrendű ciklikus csoport.

4.13.10. Következmény

Minden prímhatványrendű csoport feloldható.

Mert a lebontáskor keletkező egyszerűek prímhatványrendűek.

Prímhatványrendű csoportok

Cauchy, Sylow, 1840–80: prímhatványrendű csoportok.

Lásd jegyzet, 4.11 szakasz.

4.11.5. Következmény (NB)

Ha egy prímhatványrendű csoport egyszerű, akkor az prímrendű ciklikus csoport.

4.13.10. Következmény

Minden prímhatványrendű csoport feloldható.

Mert a lebontáskor keletkező egyszerűek prímhatványrendűek.
Jelentősége a geometriai szerkeszthetőség elméletében (6.8. Szakasz).

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok,

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek

Legyen X egy 24 elemű halmaz.

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek

Legyen X egy 24 elemű halmaz. Ki akarunk választani nyolcelemű részhalmazokat úgy,

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek

Legyen X egy 24 elemű halmaz. Ki akarunk választani nyolcelemű részhalmazokat úgy, hogy X minden ötelemű részhalmaza pontosan egyben legyen benne:

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek

Legyen X egy 24 elemű halmaz. Ki akarunk választani nyolcelemű részhalmazokat úgy, hogy X minden ötelemű részhalmaza pontosan egyben legyen benne: Steiner-rendszer.

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek

Legyen X egy 24 elemű halmaz. Ki akarunk választani nyolcelemű részhalmazokat úgy, hogy X minden ötelemű részhalmaza pontosan egyben legyen benne: Steiner-rendszer. Lényegében csak egyféleképpen lehet megcsinálni.

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek

Legyen X egy 24 elemű halmaz. Ki akarunk választani nyolcelemű részhalmazokat úgy, hogy X minden ötelemű részhalmaza pontosan egyben legyen benne: Steiner-rendszer. Lényegében csak egyféleképpen lehet megcsinálni.

M_{24} ennek a szimmetriacsoportja.

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek

Legyen X egy 24 elemű halmaz. Ki akarunk választani nyolcelemű részhalmazokat úgy, hogy X minden ötelemű részhalmaza pontosan egyben legyen benne: Steiner-rendszer. Lényegében csak egyféleképpen lehet megcsinálni.

M_{24} ennek a szimmetriacsoportja.
M_{23} ebben egy pont stabilizátora,

A Mathieu-csoportok

Mathieu, 1880 körül felfedezett 5 új egyszerű csoportot.
Jelük: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

A síkon az egyenesek részhalmazok, és bármely két pont pontosan egy egyenesen van rajta.

Általánosítás: blokkrendszerek

Legyen X egy 24 elemű halmaz. Ki akarunk választani nyolcelemű részhalmazokat úgy, hogy X minden ötelemű részhalmaza pontosan egyben legyen benne: Steiner-rendszer. Lényegében csak egyféleképpen lehet megcsinálni.

M_{24} ennek a szimmetriacsoportja.
M_{23} ebben egy pont stabilizátora, M_{22} az M_{23}-ban stabilizátor.

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be.

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét.

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét. A mátrixok elemei komplex számok,

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét. A mátrixok elemei komplex számok, jól lehet számolni velük:

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét. A mátrixok elemei komplex számok, jól lehet számolni velük: reprezentációelmélet.

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét. A mátrixok elemei komplex számok, jól lehet számolni velük: reprezentációelmélet.

4.13.11. Burnside „kétprímes” tétele

Ha a G véges egyszerű csoport rendjének legfeljebb két különböző prímosztója van, akkor az prímrendű ciklikus.

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét. A mátrixok elemei komplex számok, jól lehet számolni velük: reprezentációelmélet.

4.13.11. Burnside „kétprímes" tétele

Ha a G véges egyszerű csoport rendjének legfeljebb két különböző prímosztója van, akkor az prímrendű ciklikus.

Szellemes bizonyítás,

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét. A mátrixok elemei komplex számok, jól lehet számolni velük: reprezentációelmélet.

4.13.11. Burnside „kétprímes” tétele

Ha a G véges egyszerű csoport rendjének legfeljebb két különböző prímosztója van, akkor az prímrendű ciklikus.

Szellemes bizonyítás, az elmélet felépítésével együtt 30 oldal.

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét. A mátrixok elemei komplex számok, jól lehet számolni velük: reprezentációelmélet.

4.13.11. Burnside „kétprímes" tétele

Ha a G véges egyszerű csoport rendjének legfeljebb két különböző prímosztója van, akkor az prímrendű ciklikus.

Szellemes bizonyítás, az elmélet felépítésével együtt 30 oldal.

Következmény

Ha $|G| = p^a q^b$ (p, q prímek),

Burnside kétprímes tétele

Burnside, Frobenius: áttörés 1900 táján.

Ha G csoport, akkor vegyük a homomorfizmusait $\mathrm{GL}(n, \mathbb{C})$-be. Ezek megfogják G szerkezetét. A mátrixok elemei komplex számok, jól lehet számolni velük: reprezentációelmélet.

4.13.11. Burnside „kétprímes" tétele

Ha a G véges egyszerű csoport rendjének legfeljebb két különböző prímosztója van, akkor az prímrendű ciklikus.

Szellemes bizonyítás, az elmélet felépítésével együtt 30 oldal.

Következmény

Ha $|G| = p^a q^b$ (p, q prímek), akkor G feloldható.

Páratlan rendű csoportok

Suzuki, Feit, Thompson: 1963.

Páratlan rendű csoportok

Suzuki, Feit, Thompson: 1963.
Csoportelmélet év az Egyesült Államokban.

Páratlan rendű csoportok

Suzuki, Feit, Thompson: 1963.
Csoportelmélet év az Egyesült Államokban.

4.13.12. Feit–Thompson-tétel

Ha a G véges egyszerű csoport rendje páratlan, akkor az prímrendű ciklikus.

Páratlan rendű csoportok

Suzuki, Feit, Thompson: 1963.
Csoportelmélet év az Egyesült Államokban.

4.13.12. Feit–Thompson-tétel

Ha a G véges egyszerű csoport rendje páratlan, akkor az prímrendű ciklikus.

Számos elméletet kellett kidolgozni hozzá.

Páratlan rendű csoportok

Suzuki, Feit, Thompson: 1963.
Csoportelmélet év az Egyesült Államokban.

4.13.12. Feit–Thompson-tétel

Ha a G véges egyszerű csoport rendje páratlan, akkor az prímrendű ciklikus.

Számos elméletet kellett kidolgozni hozzá.
Nagyon nehéz bizonyítás, körülbelül 250 oldal.

Páratlan rendű csoportok

Suzuki, Feit, Thompson: 1963.
Csoportelmélet év az Egyesült Államokban.

4.13.12. Feit–Thompson-tétel

Ha a G véges egyszerű csoport rendje páratlan, akkor az prímrendű ciklikus.

Számos elméletet kellett kidolgozni hozzá.
Nagyon nehéz bizonyítás, körülbelül 250 oldal.
Használja a reprezentációelméletet is.

Páratlan rendű csoportok

Suzuki, Feit, Thompson: 1963.
Csoportelmélet év az Egyesült Államokban.

4.13.12. Feit–Thompson-tétel

Ha a G véges egyszerű csoport rendje páratlan, akkor az prímrendű ciklikus.

Számos elméletet kellett kidolgozni hozzá.
Nagyon nehéz bizonyítás, körülbelül 250 oldal.
Használja a reprezentációelméletet is.

Következmény

Minden páratlan rendű véges csoport feloldható.

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye,

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye,
a bizonyítás körülbelül 10000 oldal.

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye,
a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye,
a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja

18 végtelen sorozat.

A klasszifikáció

Sok matematikus összefogásával, 1982-re sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye, a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja

18 végtelen sorozat.

$\mathbb{Z}_p^+$, ahol p prím az első sorozat.

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye,
a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja

18 végtelen sorozat.
$\mathbb{Z}_p^+$, ahol p prím az első sorozat.
A_n (alternáló csoport), ha $n \geq 5$ a második sorozat.

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye,
a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja

18 végtelen sorozat.
$\mathbb{Z}_p^+$, ahol p prím az első sorozat.
A_n (alternáló csoport), ha $n \geq 5$ a második sorozat.
A többi 16 sorozat a geometriából származó,
mátrixokkal leírható csoportokból áll (pl. unitér mátrixok).

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye,
a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja

18 végtelen sorozat.
$\mathbb{Z}_p^+$, ahol p prím az első sorozat.
A_n (alternáló csoport), ha $n \geq 5$ a második sorozat.
A többi 16 sorozat a geometriából származó,
mátrixokkal leírható csoportokból áll (pl. unitér mátrixok).
26 sporadikus egyszerű csoport:

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye,
a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja

18 végtelen sorozat.
$\mathbb{Z}_p^+$, ahol p prím az első sorozat.
A_n (alternáló csoport), ha $n \geq 5$ a második sorozat.
A többi 16 sorozat a geometriából származó,
mátrixokkal leírható csoportokból áll (pl. unitér mátrixok).
26 sporadikus egyszerű csoport: amik nem illenek bele
a sorozatokba.

A klasszifikáció

Sok matematikus összefogásával, 1982-re sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye, a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja

18 végtelen sorozat.
$\mathbb{Z}_p^+$, ahol p prím az első sorozat.
A_n (alternáló csoport), ha $n \geq 5$ a második sorozat.
A többi 16 sorozat a geometriából származó, mátrixokkal leírható csoportokból áll (pl. unitér mátrixok).
26 sporadikus egyszerű csoport: amik nem illenek bele a sorozatokba. Például az öt Mathieu-csoport sporadikus.

A klasszifikáció

Sok matematikus összefogásával, 1982-re
sikerült megtalálni az összes véges egyszerű csoportot.

Az emberiség egyik csúcsteljesítménye,
a bizonyítás körülbelül 10000 oldal.

A véges egyszerű csoportok klasszifikációja

18 végtelen sorozat.
$\mathbb{Z}_p^+$, ahol p prím az első sorozat.
A_n (alternáló csoport), ha $n \geq 5$ a második sorozat.
A többi 16 sorozat a geometriából származó,
mátrixokkal leírható csoportokból áll (pl. unitér mátrixok).
26 sporadikus egyszerű csoport: amik nem illenek bele
a sorozatokba. Például az öt Mathieu-csoport sporadikus.

Számos alkalmazás az algebrán kívül is.

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai:

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168,

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360,

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504,

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660,

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, . . .

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster).

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982).

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

azaz körülbelül $8.08 \cdot 10^{53}$.

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

azaz körülbelül $8.08 \cdot 10^{53}$. Prímtényezős felbontása:

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

azaz körülbelül $8.08 \cdot 10^{53}$. Prímtényezős felbontása:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

azaz körülbelül $8.08 \cdot 10^{53}$. Prímtényezős felbontása:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Ez nagyságrendekkel több, mint a föld atomjainak,

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

azaz körülbelül $8.08 \cdot 10^{53}$. Prímtényezős felbontása:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Ez nagyságrendekkel több, mint a föld atomjainak, vagy az ősrobbanástól mostanáig eltelt nanoszekundumoknak a száma.

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

azaz körülbelül $8.08 \cdot 10^{53}$. Prímtényezős felbontása:

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Ez nagyságrendekkel több, mint a föld atomjainak, vagy az ősrobbanástól mostanáig eltelt nanoszekundumoknak a száma. Vagyis számítógépben nem fér el például a szorzástáblája.

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

azaz körülbelül $8.08 \cdot 10^{53}$. Prímtényezős felbontása:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Ez nagyságrendekkel több, mint a föld atomjainak, vagy az ősrobbanástól mostanáig eltelt nanoszekundumoknak a száma. Vagyis számítógépben nem fér el például a szorzástáblája.

A véges egyszerű csoportokról további táblázatok találhatók a jegyzet T. Függelékében.

A Szörnyeteg

A legkisebb nemkommutatív egyszerű csoport a 60 elemű A_5.
A következők elemszámai: 168, 360, 504, 660, 1092, ...

A legnagyobb sporadikus egyszerű csoport a Szörnyeteg (Monster). Felfeldezője Fisher és Griess (1982). Elemszáma:

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

azaz körülbelül $8.08 \cdot 10^{53}$. Prímtényezős felbontása:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Ez nagyságrendekkel több, mint a föld atomjainak, vagy az ősrobbanástól mostanáig eltelt nanoszekundumoknak a száma. Vagyis számítógépben nem fér el például a szorzástáblája.

A véges egyszerű csoportokról további táblázatok találhatók a jegyzet T. Függelékében.
Csoportelméleti fogalmak összefoglaló ábrája: 543. oldal