Algebra2, alapszint

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
ewkiss@cs.elte.hu

16. előadás

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által generált altér elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által **generált altér** elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok. Jele $\langle v_1, \ldots, v_n \rangle$.

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által
generált altér elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.
Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a legszűkebb altér, ami $v_1, \ldots, v_n$-et tartalmazza.

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által generált altér elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.
Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a legszűkebb altér, ami $v_1, \ldots, v_n$-et tartalmazza. Azaz minden W altérre, ha $v_1, \ldots, v_n \in W$

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által generált altér elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.
Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a legszűkebb altér, ami $v_1, \ldots, v_n$-et tartalmazza. Azaz minden W altérre, ha $v_1, \ldots, v_n \in W$ akkor $\langle v_1, \ldots, v_n \rangle \subseteq W$.

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által **generált altér** elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.
Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a **legszűkebb** altér, ami $v_1, \ldots, v_n$-et tartalmazza. Azaz minden W altérre, ha $v_1, \ldots, v_n \in W$ akkor $\langle v_1, \ldots, v_n \rangle \subseteq W$.

Emlékeztető

Ha G csoport, akkor a $g \in G$ elem által **generált részcsoport** elemei a g^n alakú elemek (ahol n egész).

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által generált altér elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.
Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a legszűkebb altér, ami $v_1, \ldots, v_n$-et tartalmazza. Azaz minden W altérre, ha $v_1, \ldots, v_n \in W$ akkor $\langle v_1, \ldots, v_n \rangle \subseteq W$.

Emlékeztető

Ha G csoport, akkor a $g \in G$ elem által generált részcsoport elemei a g^n alakú elemek (ahol n egész).
Jele $\langle g \rangle$.

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által generált altér elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.
Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a legszűkebb altér, ami $v_1, \ldots, v_n$-et tartalmazza. Azaz minden W altérre, ha $v_1, \ldots, v_n \in W$ akkor $\langle v_1, \ldots, v_n \rangle \subseteq W$.

Emlékeztető

Ha G csoport, akkor a $g \in G$ elem által generált részcsoport elemei a g^n alakú elemek (ahol n egész).
Jele $\langle g \rangle$.
Ez a legszűkebb részcsoport, ami a g-t tartalmazza.

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által generált altér elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.
Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a legszűkebb altér, ami $v_1, \ldots, v_n$-et tartalmazza. Azaz minden W altérre, ha $v_1, \ldots, v_n \in W$ akkor $\langle v_1, \ldots, v_n \rangle \subseteq W$.

Emlékeztető

Ha G csoport, akkor a $g \in G$ elem által generált részcsoport elemei a g^n alakú elemek (ahol n egész).
Jele $\langle g \rangle$.
Ez a legszűkebb részcsoport, ami a g-t tartalmazza. Azaz minden H részcsoportra, ha $g \in H$,

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által generált altér elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.
Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a legszűkebb altér, ami $v_1, \ldots, v_n$-et tartalmazza. Azaz minden W altérre, ha $v_1, \ldots, v_n \in W$ akkor $\langle v_1, \ldots, v_n \rangle \subseteq W$.

Emlékeztető

Ha G csoport, akkor a $g \in G$ elem által generált részcsoport elemei a g^n alakú elemek (ahol n egész).
Jele $\langle g \rangle$.
Ez a legszűkebb részcsoport, ami a g-t tartalmazza. Azaz minden H részcsoportra, ha $g \in H$, akkor $\langle g \rangle \subseteq H$.

Generált altér és ciklikus részcsoport

Emlékeztető

Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által generált altér elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok.
Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a legszűkebb altér, ami $v_1, \ldots, v_n$-et tartalmazza. Azaz minden W altérre, ha $v_1, \ldots, v_n \in W$ akkor $\langle v_1, \ldots, v_n \rangle \subseteq W$.

Emlékeztető

Ha G csoport, akkor a $g \in G$ elem által generált részcsoport elemei a g^n alakú elemek (ahol n egész).
Jele $\langle g \rangle$.
Ez a legszűkebb részcsoport, ami a g-t tartalmazza. Azaz minden H részcsoportra, ha $g \in H$, akkor $\langle g \rangle \subseteq H$.

Mi legyen $\langle g_1, \ldots, g_n \rangle$?

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat.

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $16 = 8 + 8 \in H$.

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $16 = 8 + 8 \in H$.
Mivel H zárt a kivonásra, $2 = 18 - 16 \in H$.

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $16 = 8 + 8 \in H$.
Mivel H zárt a kivonásra, $2 = 18 - 16 \in H$.
Mivel H zárt az összeadásra és a kivonásra, minden páros szám H-ban van

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $16 = 8 + 8 \in H$.
Mivel H zárt a kivonásra, $2 = 18 - 16 \in H$.
Mivel H zárt az összeadásra és a kivonásra, minden páros szám H-ban van (a pozitívak és a negatívak is).

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $16 = 8 + 8 \in H$.
Mivel H zárt a kivonásra, $2 = 18 - 16 \in H$.
Mivel H zárt az összeadásra és a kivonásra, minden páros szám H-ban van (a pozitívak és a negatívak is).
Ezek részcsoportot alkotnak, több számot nem kell bevenni.

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $16 = 8 + 8 \in H$.
Mivel H zárt a kivonásra, $2 = 18 - 16 \in H$.
Mivel H zárt az összeadásra és a kivonásra, minden páros szám H-ban van (a pozitívak és a negatívak is).
Ezek részcsoportot alkotnak, több számot nem kell bevenni.

Vagyis a 18 és 26 számokat tartalmazó legszűkebb részcsoport

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $16 = 8 + 8 \in H$.
Mivel H zárt a kivonásra, $2 = 18 - 16 \in H$.
Mivel H zárt az összeadásra és a kivonásra, minden páros szám H-ban van (a pozitívak és a negatívak is).
Ezek részcsoportot alkotnak, több számot nem kell bevenni.

Vagyis a 18 és 26 számokat tartalmazó legszűkebb részcsoport a páros számok részcsoportja.

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $16 = 8 + 8 \in H$.
Mivel H zárt a kivonásra, $2 = 18 - 16 \in H$.
Mivel H zárt az összeadásra és a kivonásra, minden páros szám H-ban van (a pozitívak és a negatívak is).
Ezek részcsoportot alkotnak, több számot nem kell bevenni.

Vagyis a 18 és 26 számokat tartalmazó legszűkebb részcsoport a páros számok részcsoportja.
Kézenfekvő: $\langle 18, 26 \rangle =$ páros számok.

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $8 = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $16 = 8 + 8 \in H$.
Mivel H zárt a kivonásra, $2 = 18 - 16 \in H$.
Mivel H zárt az összeadásra és a kivonásra, minden páros szám H-ban van (a pozitívak és a negatívak is).
Ezek részcsoportot alkotnak, több számot nem kell bevenni.

Vagyis a 18 és 26 számokat tartalmazó legszűkebb részcsoport a páros számok részcsoportja.
Kézenfekvő: $\langle 18, 26\rangle =$ páros számok.

HF: Az m és n-et tartalmazó legszűkebb részcsoport az m és n legnagyobb közös osztójának többszöröseiből áll.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$,

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$,

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$,

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$.
Ez eddig összesen 8 elem az *id* permutációval együtt.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$.
Ez eddig összesen 8 elem az *id* permutációval együtt.
Addig kellene folytatni, amíg részcsoportot nem kapunk.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$.
Ez eddig összesen 8 elem az *id* permutációval együtt.
Addig kellene folytatni, amíg részcsoportot nem kapunk.
Gyorsítás: (123) és $(12)(34)$ páros permutáció,

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$.
Ez eddig összesen 8 elem az *id* permutációval együtt.
Addig kellene folytatni, amíg részcsoportot nem kapunk.
Gyorsítás: (123) és $(12)(34)$ páros permutáció, ezért minden szorzásnál, inverzképzésnél páros permutációt kapunk.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$.
Ez eddig összesen 8 elem az id permutációval együtt.
Addig kellene folytatni, amíg részcsoportot nem kapunk.
Gyorsítás: (123) és $(12)(34)$ páros permutáció, ezért minden szorzásnál, inverzképzésnél páros permutációt kapunk.
Lagrange tétele miatt A_4-nek legalább 8 elemű részcsoportja csak maga A_4 lehet.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$.
Ez eddig összesen 8 elem az id permutációval együtt.
Addig kellene folytatni, amíg részcsoportot nem kapunk.
Gyorsítás: (123) és $(12)(34)$ páros permutáció, ezért minden szorzásnál, inverzképzésnél páros permutációt kapunk.
Lagrange tétele miatt A_4-nek legalább 8 elemű részcsoportja csak maga A_4 lehet. Ezért csak A_4-nél állhatunk le.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$.
Ez eddig összesen 8 elem az *id* permutációval együtt.
Addig kellene folytatni, amíg részcsoportot nem kapunk.
Gyorsítás: (123) és $(12)(34)$ páros permutáció, ezért minden szorzásnál, inverzképzésnél páros permutációt kapunk.
Lagrange tétele miatt A_4-nek legalább 8 elemű részcsoportja csak maga A_4 lehet. Ezért csak A_4-nél állhatunk le.

Vagyis az (123) és $(12)(34)$ permutációkat tartalmazó legszűkebb részcsoport az A_4 alternáló csoport.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és $(12)(34)$ permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, $(134) = (123)(12)(34) \in H$.
Hasonlóan $(243) = (12)(34)(123) \in H$, továbbá
$(132) = (123)^2 \in H$, $(143) = (134)^2 \in H$, $(234) = (243)^2 \in H$.
Ez eddig összesen 8 elem az *id* permutációval együtt.
Addig kellene folytatni, amíg részcsoportot nem kapunk.
Gyorsítás: (123) és $(12)(34)$ páros permutáció, ezért minden szorzásnál, inverzképzésnél páros permutációt kapunk.
Lagrange tétele miatt A_4-nek legalább 8 elemű részcsoportja csak maga A_4 lehet. Ezért csak A_4-nél állhatunk le.

Vagyis az (123) és $(12)(34)$ permutációkat tartalmazó legszűkebb részcsoport az A_4 alternáló csoport.
Kézenfekvő: $\langle(123), (12)(34)\rangle = A_4$.

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által
generált részcsoport

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által **generált részcsoport** a **legszűkebb** X-et tartalmazó részcsoportja G-nek,

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által **generált részcsoport** a **legszűkebb** X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által **generált részcsoport** a **legszűkebb** X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X elemeit,

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által **generált részcsoport** a **legszűkebb** X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X elemeit, tartalmazza az $\langle X \rangle$ részcsoportot is.

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által generált részcsoport a legszűkebb X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X elemeit, tartalmazza az $\langle X \rangle$ részcsoportot is. Az X részhalmazt G generátorrendszerének nevezzük

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által generált részcsoport a legszűkebb X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X elemeit, tartalmazza az $\langle X \rangle$ részcsoportot is. Az X részhalmazt G generátorrendszerének nevezzük ha $\langle X \rangle = G$.

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által **generált részcsoport** a **legszűkebb** X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X elemeit, tartalmazza az $\langle X \rangle$ részcsoportot is. Az X részhalmazt G **generátorrendszerének** nevezzük (illetve azt mondjuk, hogy X **generálja** G-t), ha $\langle X \rangle = G$.

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által **generált részcsoport** a **legszűkebb** X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X elemeit, tartalmazza az $\langle X \rangle$ részcsoportot is. Az X részhalmazt G **generátorrendszerének** nevezzük (illetve azt mondjuk, hogy X **generálja** G-t), ha $\langle X \rangle = G$.

4.6.7. Állítás

A generált részcsoport egyértelműen létezik.

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által generált részcsoport a legszűkebb X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X elemeit, tartalmazza az $\langle X \rangle$ részcsoportot is. Az X részhalmazt G generátorrendszerének nevezzük (illetve azt mondjuk, hogy X generálja G-t), ha $\langle X \rangle = G$.

4.6.7. Állítás

A generált részcsoport egyértelműen létezik.
Úgy kapható, mint az X-et tartalmazó részcsoportok metszete.

Generált részcsoport

4.6.3. Definíció

Tetszőleges G csoport esetén az $X \subseteq G$ által generált részcsoport a legszűkebb X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X elemeit, tartalmazza az $\langle X \rangle$ részcsoportot is. Az X részhalmazt G generátorrendszerének nevezzük (illetve azt mondjuk, hogy X generálja G-t), ha $\langle X \rangle = G$.

4.6.7. Állítás

A generált részcsoport egyértelműen létezik.
Úgy kapható, mint az X-et tartalmazó részcsoportok metszete.

Ennek bizonyítását alapszinten nem kell megemészteni.

A generált részcsoport elemei

4.6.1. Állítás

Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$.

A generált részcsoport elemei

4.6.1. Állítás

Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ elemek L halmazát,

A generált részcsoport elemei

4.6.1. Állítás

Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ elemek L halmazát, ahol m_i egész számok.

A generált részcsoport elemei

4.6.1. Állítás

Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ elemek L halmazát, ahol m_i egész számok. Ekkor L az A legszűkebb olyan részcsoportja, amely a $g_1, \ldots, g_n$ elemeket tartalmazza.

A generált részcsoport elemei

4.6.1. Állítás

Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ elemek L halmazát, ahol m_i egész számok. Ekkor L az A legszűkebb olyan részcsoportja, amely a $g_1, \ldots, g_n$ elemeket tartalmazza.

4.6.8. Tétel

Legyen G csoport és $X \subseteq G$.

A generált részcsoport elemei

4.6.1. Állítás

Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ elemek L halmazát, ahol m_i egész számok. Ekkor L az A legszűkebb olyan részcsoportja, amely a $g_1, \ldots, g_n$ elemeket tartalmazza.

4.6.8. Tétel

Legyen G csoport és $X \subseteq G$. Ekkor $\langle X \rangle$ a G azon elemeiből áll,

A generált részcsoport elemei

4.6.1. Állítás

Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ elemek L halmazát, ahol m_i egész számok. Ekkor L az A legszűkebb olyan részcsoportja, amely a $g_1, \ldots, g_n$ elemeket tartalmazza.

4.6.8. Tétel

Legyen G csoport és $X \subseteq G$. Ekkor $\langle X \rangle$ a G azon elemeiből áll, melyek fölírhatók az X elemeiből és azok inverzeiből képzett akárhány tényezős szorzatként

A generált részcsoport elemei

4.6.1. Állítás

Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ elemek L halmazát, ahol m_i egész számok. Ekkor L az A legszűkebb olyan részcsoportja, amely a $g_1, \ldots, g_n$ elemeket tartalmazza.

4.6.8. Tétel

Legyen G csoport és $X \subseteq G$. Ekkor $\langle X \rangle$ a G azon elemeiből áll, melyek fölírhatók az X elemeiből és azok inverzeiből képzett akárhány tényezős szorzatként (X minden eleme többször is felhasználható egy ilyen szorzatban).

A generált részcsoport elemei

4.6.1. Állítás

Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ elemek L halmazát, ahol m_i egész számok. Ekkor L az A legszűkebb olyan részcsoportja, amely a $g_1, \ldots, g_n$ elemeket tartalmazza.

4.6.8. Tétel

Legyen G csoport és $X \subseteq G$. Ekkor $\langle X \rangle$ a G azon elemeiből áll, melyek fölírhatók az X elemeiből és azok inverzeiből képzett akárhány tényezős szorzatként (X minden eleme többször is felhasználható egy ilyen szorzatban).

Ezek bizonyítását alapszinten nem kell tudni.

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?

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

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?

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

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

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?

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

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

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 $12 = [6, 4]$.

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?
$g^1 = (2,3)$, $g^2 = (4,4)$, $g^3 = (8,2)$, $g^4 = (7,1)$,
$g^5 = (5,3)$, $g^6 = (1,4)$, $g^7 = (2,2)$, $g^8 = (4,1)$,
$g^9 = (8,3)$, $g^{10} = (7,4)$, $g^{11} = (5,2)$, $g^{12} = (1,1)$.
Vagyis g rendje 12. De $o_9(2) = 6$, $o_5(3) = 4$ és $12 = [6,4]$.

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

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

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

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

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

A bizonyítást alapszinten nem kell tudni.

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

4.9.9. Következmény

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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.

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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.

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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
Speciálisan adódik, hogy a φ Euler-függvény multiplikatív.
Emlékeztető: A g szám primitív gyök modulo n,

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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
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

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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
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 bizonyítás egy része lesz jövőre, most nem kell tudni.

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

4.9.9. Következmény

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

A bizonyítást (lásd jegyzet) alapszinten nem kell tudni.
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 bizonyítás egy része lesz jövőre, most nem kell tudni.
Lásd a jegyzetben: 4.9.10, 4.4.33, 4.9.36.

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.