Algebraiska strukturer

Från magmor till symmetrigrupper

Jonathan Nilsson

Linköpings Universitet

Idag

- Magmor
  - Binära operationer
  - Associativitet, kommutativitet, identitetselement
  - Ett antal exempel
- Grupper
  - Symmetrigrupper
  - Frismönster
  - Tapetgrupper

Del I

Magmor

Binära operationer

Definition

En **binär operation** på en mängd M är en funktion $f : M \times M \to M$.
En mängd utrustad med en binär operation kallas för en **magma**.

Binära operationer

Definition

En **binär operation** på en mängd M är en funktion $f : M \times M \to M$.
En mängd utrustad med en binär operation kallas för en **magma**.
Normalt inför man notation och skriver t.ex. $a \star b$ istället för $f(a, b)$.

Binära operationer

Definition

En **binär operation** på en mängd M är en funktion $f : M \times M \to M$.
En mängd utrustad med en binär operation kallas för en **magma**.
Normalt inför man notation och skriver t.ex. $a \star b$ istället för $f(a, b)$.

Exempel:

- $(\mathbb{N}, +)$, de naturliga talen utrustade med addition är en magma.

Binära operationer

Definition

En **binär operation** på en mängd M är en funktion $f : M \times M \to M$.
En mängd utrustad med en binär operation kallas för en **magma**.
Normalt inför man notation och skriver t.ex. $a \star b$ istället för $f(a, b)$.

Exempel:

- $(\mathbb{N}, +)$, de naturliga talen utrustade med addition är en magma.
- $(\mathbb{R}, \cdot)$, de reella talen med multiplikation är en magma.

Binära operationer

Definition

En **binär operation** på en mängd M är en funktion $f : M \times M \to M$.
En mängd utrustad med en binär operation kallas för en **magma**.
Normalt inför man notation och skriver t.ex. $a \star b$ istället för $f(a, b)$.

Exempel:

- $(\mathbb{N}, +)$, de naturliga talen utrustade med addition är en magma.
- $(\mathbb{R}, \cdot)$, de reella talen med multiplikation är en magma.
- $(\mathbb{N}, -)$, de naturliga talen utrustade med subtraktion är *inte* en magma, operationen är inte sluten, exempelvis är $3 - 7 \notin \mathbb{N}$.

Binära operationer

Definition

En **binär operation** på en mängd M är en funktion $f : M \times M \to M$.
En mängd utrustad med en binär operation kallas för en **magma**.
Normalt inför man notation och skriver t.ex. $a \star b$ istället för $f(a, b)$.

Exempel:

- $(\mathbb{N}, +)$, de naturliga talen utrustade med addition är en magma.
- $(\mathbb{R}, \cdot)$, de reella talen med multiplikation är en magma.
- $(\mathbb{N}, -)$, de naturliga talen utrustade med subtraktion är *inte* en magma, operationen är inte sluten, exempelvis är $3 - 7 \notin \mathbb{N}$.
- $(\mathbb{R}, /)$, de reella talen med division är *inte* en magma, $\frac{5}{0}$ är odefinierat.

Sten-sax-påse magman

$M = \Big\{$  ,  ,  $\Big\}$.

Sten-sax-påse magman

$M = \{$  ,  ,  $\}$.

Vi definierar en binär operatinen $\star$ på M genom att bestämma att produkten av två element är vinnaren i sten-sax-påse, t.ex.  $\star$  $=$  .

Det kan ju också bli oavgjort, så vi definierar även  $\star$  $=$  och så vidare.

Sten-sax-påse magman

$M = \{$  $\}$.

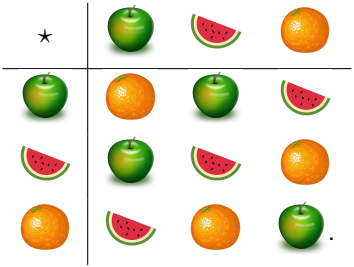
Vi definierar en binär operatinen $\star$ på M genom att bestämma att produkten av två element är vinnaren i sten-sax-påse, t.ex.  $\star$  $=$  .

Det kan ju också bli oavgjort, så vi definierar även  $\star$  $=$  och så vidare.

$\star$			
			
			
			

En magma av frukt

Låt **fruktmagman** vara $(\{$🍏, 🍉, 🍊$\}, \star)$ där $\star$ beskrivs av multiplikationstabellen nedan



.

Solkrämsmagman

Om jag blandar solskyddsfaktor 20 med solskyddsfaktor 30 i lika delar, vilken solskyddsfaktor får blandningen?

#

Solkrämsmagman

Om jag blandar solskyddsfaktor 20 med solskyddsfaktor 30 i lika delar, vilken solskyddsfaktor får blandningen?

Medelvärdet av $\frac{1}{30}$ och $\frac{1}{20}$ är $\frac{1}{24}$, så svaret är 24.

Solkrämsmagman

Om jag blandar solskyddsfaktor 20 med solskyddsfaktor 30 i lika delar, vilken solskyddsfaktor får blandningen?

Medelvärdet av $\frac{1}{30}$ och $\frac{1}{20}$ är $\frac{1}{24}$, så svaret är 24.
Vi definierar en binär operation på de positiva reella talen: $x\#y = \frac{1}{\frac{\frac{1}{x}+\frac{1}{y}}{2}}$, och kallar $(\mathbb{R}^+, \#)$ för **solkrämsmagman**.

Egenskaper

Vad blir  $\star$  $\star$  ?

Egenskaper

Vad blir  $\star$  $\star$  ?

 $\star$ ( $\star$ ) $\neq$ ( $\star$ ) $\star$ 

Associativitet

Definition

En magma $(M, \star)$ kallas **associativ** om $(a \star b) \star c = a \star (b \star c)$ för alla $a, b, c \in M$. En associativ magma kallas för en **halvgrupp**.

Associativitet

Definition

En magma $(M, \star)$ kallas **associativ** om $(a \star b) \star c = a \star (b \star c)$ för alla $a, b, c \in M$. En associativ magma kallas för en **halvgrupp**.

- I en associativ magma behöver man inte sätta ut parenteser, vi kan skriva $a \star b \star c$ eftersom vi får samma resultat oavsätt hur vi sätter ut parenteser.

Associativitet

Definition

En magma $(M, \star)$ kallas **associativ** om $(a \star b) \star c = a \star (b \star c)$ för alla $a, b, c \in M$. En associativ magma kallas för en **halvgrupp**.

- I en associativ magma behöver man inte sätta ut parenteser, vi kan skriva $a \star b \star c$ eftersom vi får samma resultat oavsätt hur vi sätter ut parenteser.
- Sten-sax-påse magman är *inte* associativ

Associativitet

Definition

En magma $(M, \star)$ kallas **associativ** om $(a \star b) \star c = a \star (b \star c)$ för alla $a, b, c \in M$. En associativ magma kallas för en **halvgrupp**.

- I en associativ magma behöver man inte sätta ut parenteser, vi kan skriva $a \star b \star c$ eftersom vi får samma resultat oavsätt hur vi sätter ut parenteser.
- Sten-sax-påse magman är *inte* associativ
- Fruktmagman är associativ

Associativitet

Definition

En magma $(M, \star)$ kallas **associativ** om $(a \star b) \star c = a \star (b \star c)$ för alla $a, b, c \in M$. En associativ magma kallas för en **halvgrupp**.

- I en associativ magma behöver man inte sätta ut parenteser, vi kan skriva $a \star b \star c$ eftersom vi får samma resultat oavsätt hur vi sätter ut parenteser.
- Sten-sax-påse magman är *inte* associativ
- Fruktmagman är associativ
- Solkrämsmagman är inte associativ

Associativitet

Definition

En magma $(M, \star)$ kallas **associativ** om $(a \star b) \star c = a \star (b \star c)$ för alla $a, b, c \in M$. En associativ magma kallas för en **halvgrupp**.

- I en associativ magma behöver man inte sätta ut parenteser, vi kan skriva $a \star b \star c$ eftersom vi får samma resultat oavsätt hur vi sätter ut parenteser.
- Sten-sax-påse magman är *inte* associativ
- Fruktmagman är associativ
- Solkrämsmagman är inte associativ
- $(\mathbb{N}, +)$ är associativ

Associativitet

Definition

En magma $(M, \star)$ kallas **associativ** om $(a \star b) \star c = a \star (b \star c)$ för alla $a, b, c \in M$. En associativ magma kallas för en **halvgrupp**.

- I en associativ magma behöver man inte sätta ut parenteser, vi kan skriva $a \star b \star c$ eftersom vi får samma resultat oavsätt hur vi sätter ut parenteser.
- Sten-sax-påse magman är *inte* associativ
- Fruktmagman är associativ
- Solkrämsmagman är inte associativ
- $(\mathbb{N}, +)$ är associativ
- $(\mathbb{Z}, -)$ är *inte* associativ, exempelvis är $(8 - 3) - 2 \neq 8 - (3 - 2)$

Kommutativitet

Definition

En magma $(M, \star)$ kallas **kommutativ** eller **abelsk** om $a \star b = b \star a$ för alla $a, b \in M$.

Kommutativitet

Definition

En magma $(M, \star)$ kallas **kommutativ** eller **abelsk** om $a \star b = b \star a$ för alla $a, b \in M$.

- Sten-sax-påse magman, frukt-magman, och solkrämsmagman är kommutativa

Kommutativitet

Definition

En magma $(M, \star)$ kallas **kommutativ** eller **abelsk** om $a \star b = b \star a$ för alla $a, b \in M$.

- Sten-sax-påse magman, frukt-magman, och solkrämsmagman är kommutativa
- $(\mathbb{N}, +)$ är kommutativ

Kommutativitet

Definition

En magma $(M, \star)$ kallas **kommutativ** eller **abelsk** om $a \star b = b \star a$ för alla $a, b \in M$.

- Sten-sax-påse magman, frukt-magman, och solkrämsmagman är kommutativa
- $(\mathbb{N}, +)$ är kommutativ
- $(\mathbb{Z}, -)$ är *inte* kommutativ, exempelvis är $5 - 3 \neq 3 - 5$

Kommutativitet

Definition

En magma $(M, \star)$ kallas **kommutativ** eller **abelsk** om $a \star b = b \star a$ för alla $a, b \in M$.

- Sten-sax-påse magman, frukt-magman, och solkrämsmagman är kommutativa
- $(\mathbb{N}, +)$ är kommutativ
- $(\mathbb{Z}, -)$ är *inte* kommutativ, exempelvis är $5 - 3 \neq 3 - 5$
- Matrismultiplikation är icke-kommutativ

Moduloräkning

Vad är klockan om 1000000 timmar?

Moduloräkning

Vad är klockan om 1000000 timmar?

Om klockan är 11 nu så kan vi beräkna:
$11 + 1000000 = 1000011 = 83334 \cdot 12 + 3 \simeq 3$ så klockan är 3.

Räkning i $\mathbb{Z}_3$

Låt $\overline{1} = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$
och $\overline{2} = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$
och $\overline{3} = \{3 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

Räkning i $\mathbb{Z}_3$

Låt $\overline{1} = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$
och $\overline{2} = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$
och $\overline{3} = \{3 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$
och allmänt $\overline{n} = \{n + 3k \mid k \in \mathbb{Z}\} = \{\ldots, n - 6, n - 3, n, n + 3, n + 6, \ldots\}$

Räkning i $\mathbb{Z}_3$

Låt $\overline{1} = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$
och $\overline{2} = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$
och $\overline{3} = \{3 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

och allmänt $\overline{n} = \{n + 3k \mid k \in \mathbb{Z}\} = \{\ldots, n - 6, n - 3, n, n + 3, n + 6, \ldots\}$

Då är alltid $\overline{n}$ lika med en av dessa tre mängder. Låt nu $\mathbb{Z}_3 = \{\overline{1}, \overline{2}, \overline{3}\}$, och definiera $\overline{m} + \overline{n} = \overline{m + n}$, detta är en binär operation på $\mathbb{Z}_3$, och $(\mathbb{Z}_3, +)$ är en magma. Analogt kan vi definiera $\overline{m} \cdot \overline{n} = \overline{m \cdot n}$, och få en magma $(\mathbb{Z}_3, \cdot)$.

Räkning i $\mathbb{Z}_3$

Låt $\overline{1} = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$
och $\overline{2} = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$
och $\overline{3} = \{3 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

och allmänt $\overline{n} = \{n + 3k \mid k \in \mathbb{Z}\} = \{\ldots, n - 6, n - 3, n, n + 3, n + 6, \ldots\}$

Då är alltid $\overline{n}$ lika med en av dessa tre mängder. Låt nu $\mathbb{Z}_3 = \{\overline{1}, \overline{2}, \overline{3}\}$, och definiera $\overline{m} + \overline{n} = \overline{m + n}$, detta är en binär operation på $\mathbb{Z}_3$, och $(\mathbb{Z}_3, +)$ är en magma. Analogt kan vi definiera $\overline{m} \cdot \overline{n} = \overline{m \cdot n}$, och få en magma $(\mathbb{Z}_3, \cdot)$.

$+$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{1}$
$\overline{2}$	$\overline{3}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Identitetselement

Definition

Låt $(M, \star)$ vara en magma. Ett element $e \in M$ som uppfyller $e \star x = x$ och $x \star e = x$ för alla $x \in M$ kallas för ett **identitetselement** i magman.

Identitetselement

Definition

Låt $(M, \star)$ vara en magma. Ett element $e \in M$ som uppfyller $e \star x = x$ och $x \star e = x$ för alla $x \in M$ kallas för ett **identitetselement** i magman.

- Har $(\mathbb{Z}, +)$ något identitetselement?

Identitetselement

Definition

Låt $(M, \star)$ vara en magma. Ett element $e \in M$ som uppfyller $e \star x = x$ och $x \star e = x$ för alla $x \in M$ kallas för ett **identitetselement** i magman.

- Har $(\mathbb{Z}, +)$ något identitetselement? Ja, 0.
- Har $(\mathbb{Z}, \cdot)$ något identitetselement?

Identitetselement

Definition

Låt $(M, \star)$ vara en magma. Ett element $e \in M$ som uppfyller $e \star x = x$ och $x \star e = x$ för alla $x \in M$ kallas för ett **identitetselement** i magman.

- Har $(\mathbb{Z}, +)$ något identitetselement? Ja, 0.
- Har $(\mathbb{Z}, \cdot)$ något identitetselement? Ja, 1.
- Har fruktmagman något identitetselement?

Identitetselement

Definition

Låt $(M, \star)$ vara en magma. Ett element $e \in M$ som uppfyller $e \star x = x$ och $x \star e = x$ för alla $x \in M$ kallas för ett **identitetselement** i magman.

- Har $(\mathbb{Z}, +)$ något identitetselement? Ja, 0.
- Har $(\mathbb{Z}, \cdot)$ något identitetselement? Ja, 1.
- Har fruktmagman något identitetselement? Ja, 🍉.
- Har sten-sax-påse-magman något identitetselement?

Identitetselement

Definition

Låt $(M, \star)$ vara en magma. Ett element $e \in M$ som uppfyller $e \star x = x$ och $x \star e = x$ för alla $x \in M$ kallas för ett **identitetselement** i magman.

- Har $(\mathbb{Z}, +)$ något identitetselement? Ja, 0.
- Har $(\mathbb{Z}, \cdot)$ något identitetselement? Ja, 1.
- Har fruktmagman något identitetselement? Ja, 🍉.
- Har sten-sax-påse-magman något identitetselement? Nej.
- Har $(\mathbb{Z}_3, +)$ något identitetselement?

Identitetselement

Definition

Låt $(M, \star)$ vara en magma. Ett element $e \in M$ som uppfyller $e \star x = x$ och $x \star e = x$ för alla $x \in M$ kallas för ett **identitetselement** i magman.

- Har $(\mathbb{Z}, +)$ något identitetselement? Ja, 0.
- Har $(\mathbb{Z}, \cdot)$ något identitetselement? Ja, 1.
- Har fruktmagman något identitetselement? Ja,  .
- Har sten-sax-påse-magman något identitetselement? Nej.
- Har $(\mathbb{Z}_3, +)$ något identitetselement? Ja, $\overline{3}$

Identitetselement

Definition

Låt $(M, \star)$ vara en magma. Ett element $e \in M$ som uppfyller $e \star x = x$ och $x \star e = x$ för alla $x \in M$ kallas för ett **identitetselement** i magman.

- Har $(\mathbb{Z}, +)$ något identitetselement? Ja, 0.
- Har $(\mathbb{Z}, \cdot)$ något identitetselement? Ja, 1.
- Har fruktmagman något identitetselement? Ja,  .
- Har sten-sax-påse-magman något identitetselement? Nej.
- Har $(\mathbb{Z}_3, +)$ något identitetselement? Ja, $\overline{3}$

Sats

En magma kan ha högst ett identitetselement.

Identitetselement

Definition

Låt $(M, \star)$ vara en magma. Ett element $e \in M$ som uppfyller $e \star x = x$ och $x \star e = x$ för alla $x \in M$ kallas för ett **identitetselement** i magman.

- Har $(\mathbb{Z}, +)$ något identitetselement? Ja, 0.
- Har $(\mathbb{Z}, \cdot)$ något identitetselement? Ja, 1.
- Har fruktmagman något identitetselement? Ja,  .
- Har sten-sax-påse-magman något identitetselement? Nej.
- Har $(\mathbb{Z}_3, +)$ något identitetselement? Ja, $\overline{3}$

Sats

En magma kan ha högst ett identitetselement.

Bevis: Om e och f både är identitetselement så gäller $e = e \star f = f$.

Grupper

Definition

En **grupp** är en associativ magma $(G, \star)$ med identitetselement e, och där varje element har en invers: för varje $x \in G$ finns det $y \in G$ så att $x \star y = e$ och $y \star x = e$.

Grupper

Definition

En **grupp** är en associativ magma $(G, \star)$ med identitetselement e, och där varje element har en invers: för varje $x \in G$ finns det $y \in G$ så att $x \star y = e$ och $y \star x = e$.

Exempel: $(\mathbb{Z}, +)$, $(\mathbb{Z}_3, +)$, och fruktmagman är grupper.
Stensakpåsemagman, solkrämsmagman, och $(\mathbb{Z}, \cdot)$ är inte grupper.

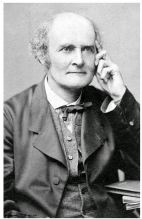
Grupper

Definition

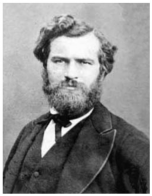
En **grupp** är en associativ magma $(G, \star)$ med identitetselement e, och där varje element har en invers: för varje $x \in G$ finns det $y \in G$ så att $x \star y = e$ och $y \star x = e$.

Exempel: $(\mathbb{Z}, +)$, $(\mathbb{Z}_3, +)$, och fruktmagman är grupper.
Stensakpåsemagman, solkrämsmagman, och $(\mathbb{Z}, \cdot)$ är inte grupper.

Évariste Galois



Arthur Cayley



Camille Jordan

Isomorfi

Två magmor som ser olika ut kan ändå ha exakt samma struktur från ett matematisk perspektiv.

Isomorfi

Två magmor som ser olika ut kan ändå ha exakt samma struktur från ett matematisk perspektiv.

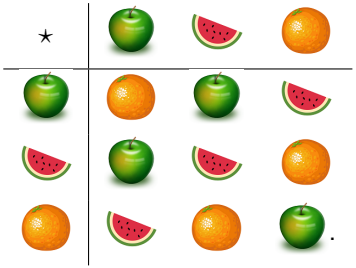
Definition

Vi säger att magmorna $(M, \star)$ och $(N, *)$ är **isomorfa** om det finns en bijektiv funktion $f : M \to N$ som bevarar gruppstrukturen:

$$f(m \star m') = f(m) * f(m') \text{ för alla } m, m' \in M$$

Exempel

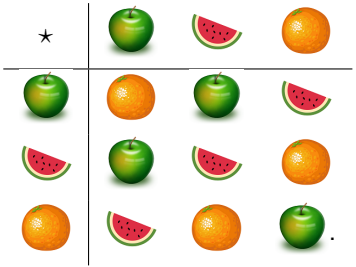
Är fruktmagman isomorf med $\mathbb{Z}_3$?



$+$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{1}$
$\overline{2}$	$\overline{3}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Exempel

Är fruktmagman isomorf med $\mathbb{Z}_3$?

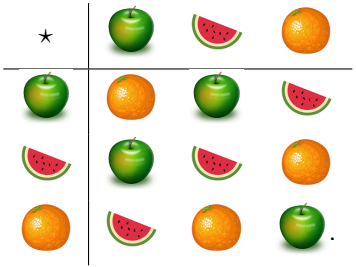


$+$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{1}$
$\overline{2}$	$\overline{3}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Låt $f($  $) = \overline{1}$, $f($  $) = \overline{2}$, $f($  $) = \overline{3}$.

Exempel

Är fruktmagman isomorf med $\mathbb{Z}_3$?



$+$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{1}$
$\overline{2}$	$\overline{3}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Låt $f($  $) = \overline{1}$, $f($  $) = \overline{2}$, $f($  $) = \overline{3}$.

Då är f en isomorfi.

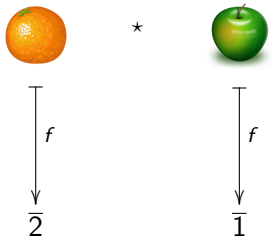
Illustration

$f(\text{  }) = \overline{1} \qquad f(\text{  }) = \overline{2} \qquad f(\text{  }) = \overline{3}.$

 $\star$ 

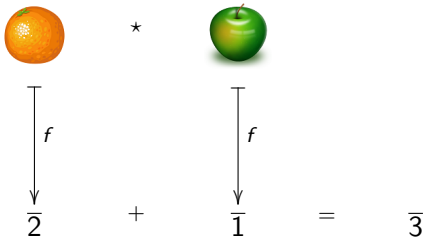
Illustration

$f(\text{🍏}) = \overline{1} \qquad f(\text{🍊}) = \overline{2} \qquad f(\text{🍉}) = \overline{3}.$



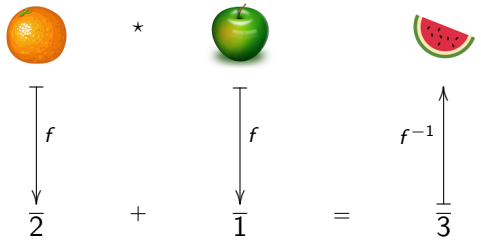
Illustration

$f(\text{🍏}) = \overline{1} \qquad f(\text{🍊}) = \overline{2} \qquad f(\text{🍉}) = \overline{3}.$



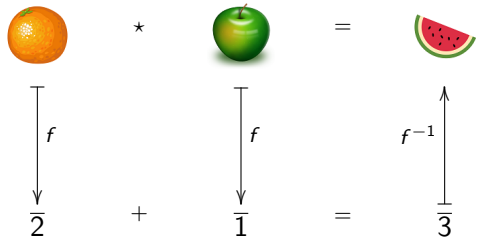
Illustration

$f(\text{🍏}) = \overline{1} \qquad f(\text{🍊}) = \overline{2} \qquad f(\text{🍉}) = \overline{3}.$



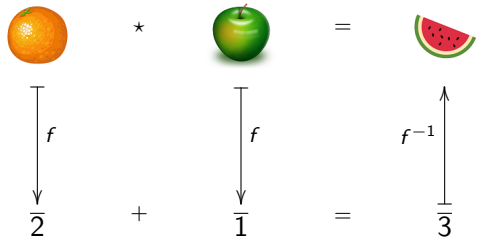
Illustration

$f(\text{🍏}) = \overline{1} \qquad f(\text{🍊}) = \overline{2} \qquad f(\text{🍉}) = \overline{3}.$



Illustration

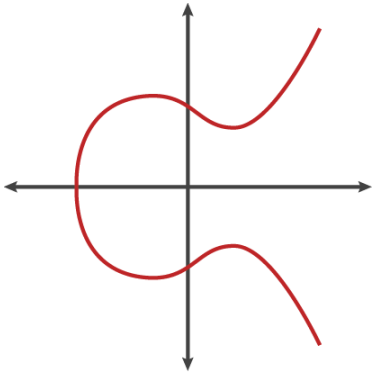
$f(\text{🍏}) = \overline{1} \qquad f(\text{🍊}) = \overline{2} \qquad f(\text{🍉}) = \overline{3}.$



Detta illustrerar att $f(\text{🍊}) + f(\text{🍏}) = f(\text{🍊} \star \text{🍏})$

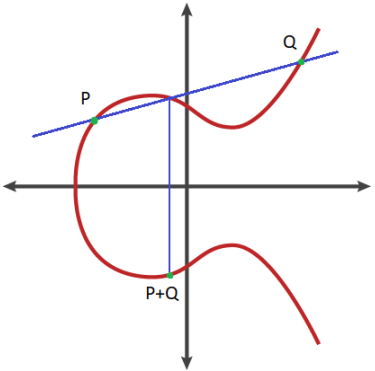
Gruppstruktur på en elliptisk kurva

Låt $\Omega = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 - x + 1\} \cup \{\infty\}$.



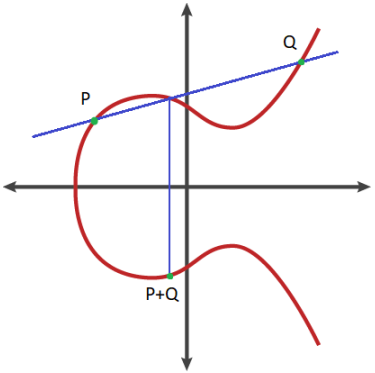
Gruppstruktur på en elliptisk kurva

Låt $\Omega = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 - x + 1\} \cup \{\infty\}$.
Vi definierar en binär operation på Ω enligt bilden: $P + Q =$ tredje skärningspunkten mellan linjen PQ och kurvan, fast speglad i x-axeln.



Gruppstruktur på en elliptisk kurva

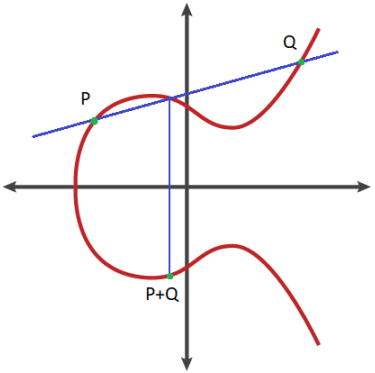
Låt $\Omega = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 - x + 1\} \cup \{\infty\}$.



Är $(\Omega, +)$ kommutativ?

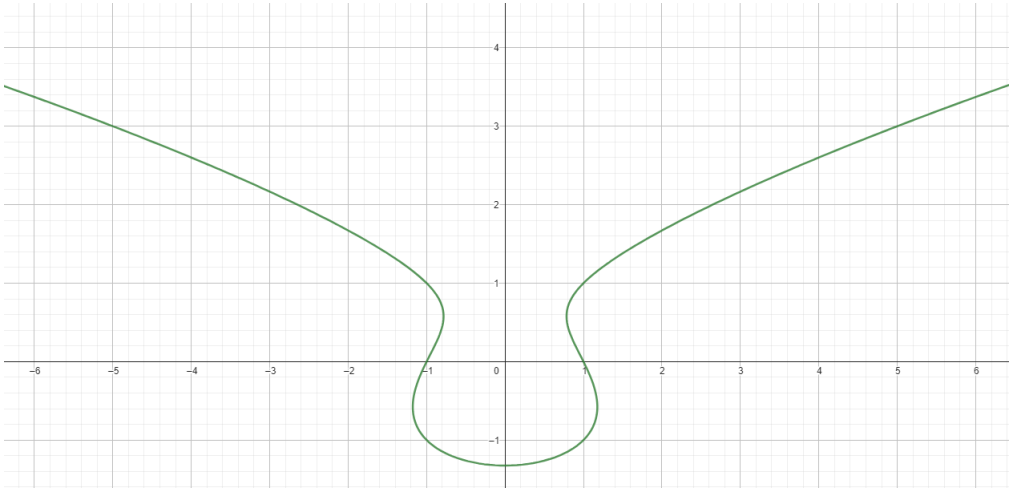
Gruppstruktur på en elliptisk kurva

Låt $\Omega = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 - x + 1\} \cup \{\infty\}$.

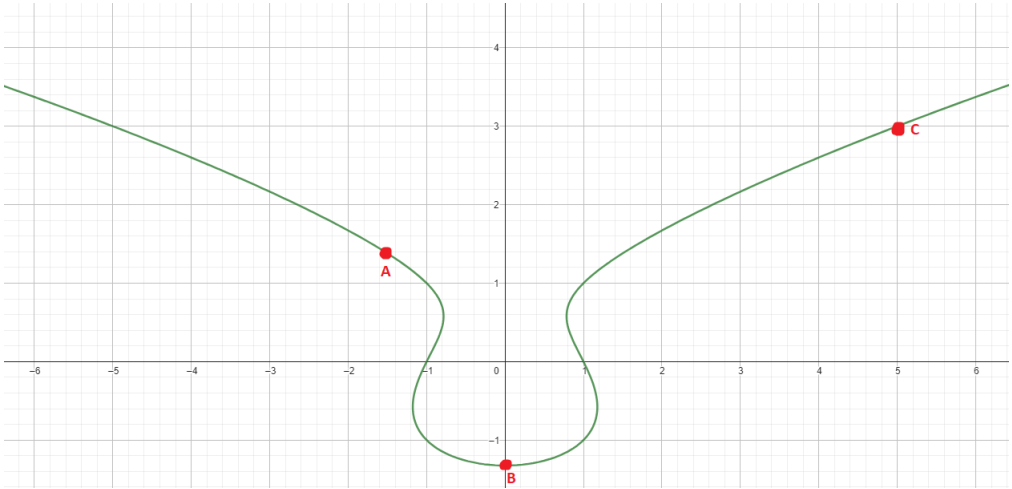


Är $(\Omega, +)$ kommutativ? Ja!

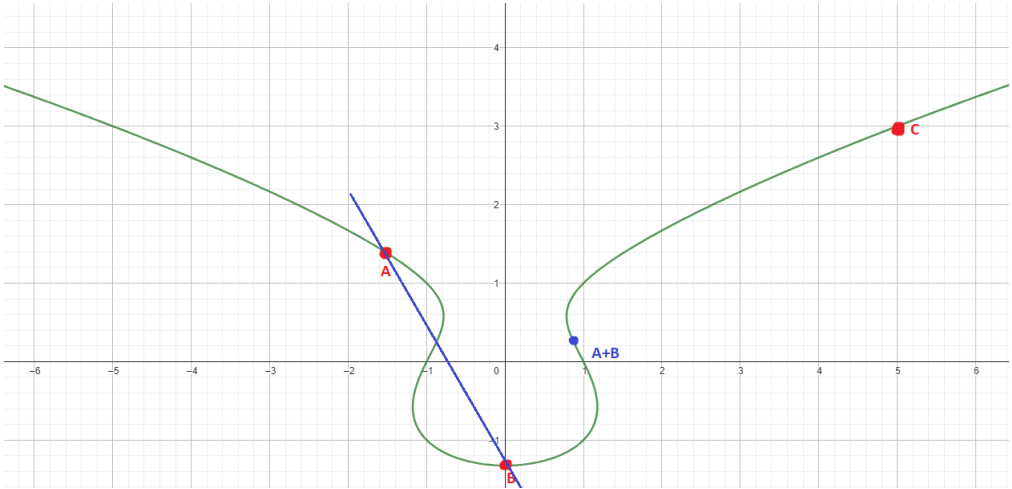
Är $(\Omega, +)$ associativ?



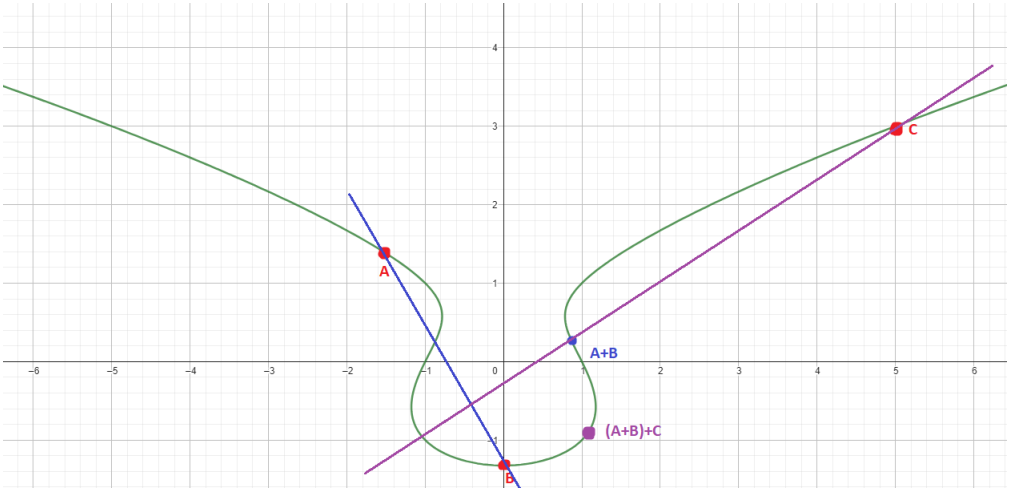
Är $(\Omega, +)$ associativ?



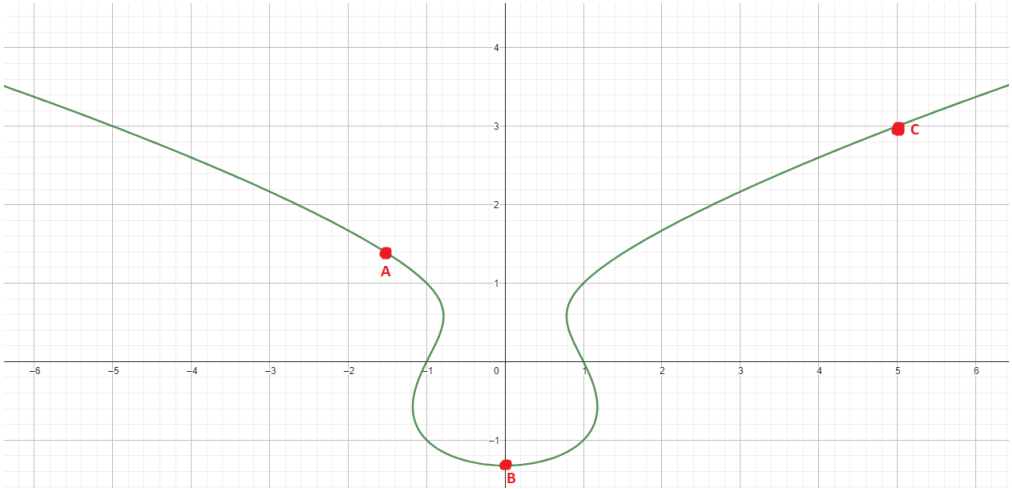
Är $(\Omega, +)$ associativ?



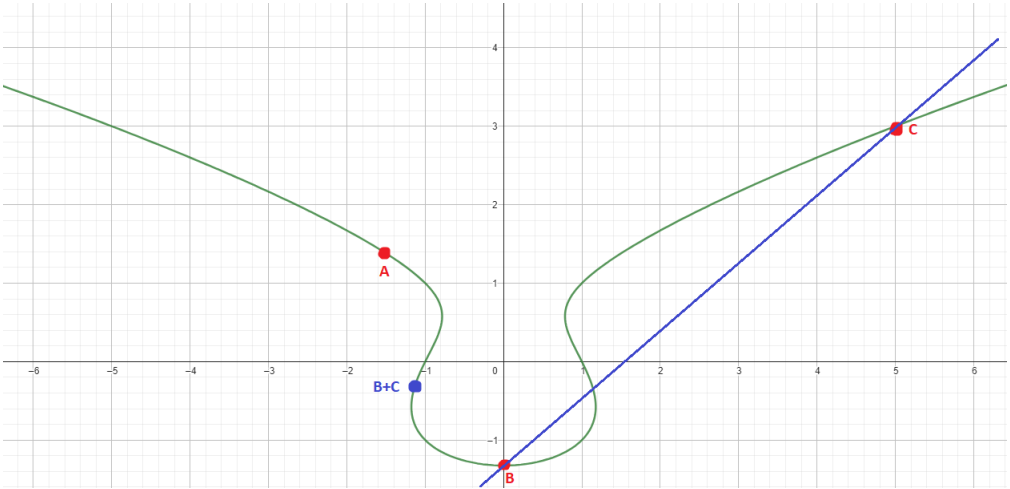
Är $(\Omega, +)$ associativ?



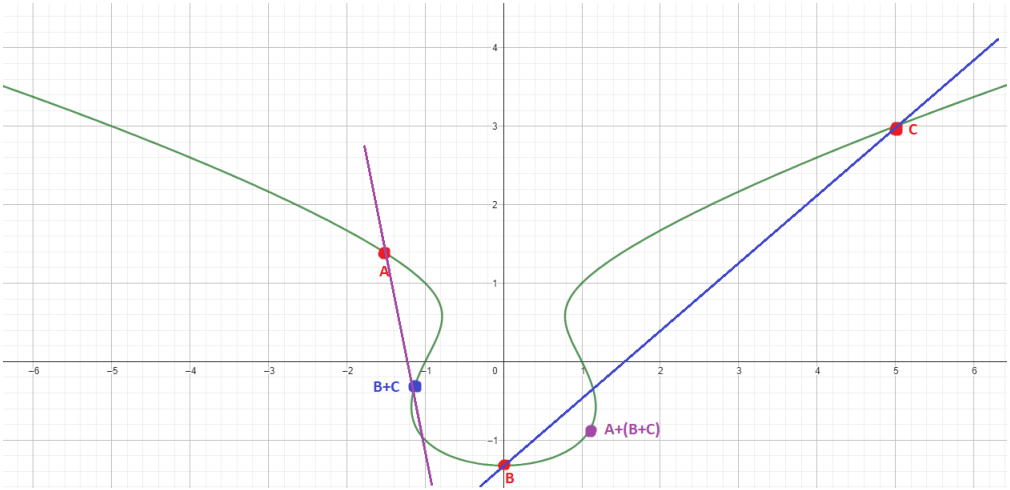
Är $(\Omega, +)$ associativ?



Är $(\Omega, +)$ associativ?



Är $(\Omega, +)$ associativ?



Ja! $(A + B) + C = A + (B + C)$

Tillämpning: kryptering med elliptiska kurvor

Jag väljer en punkt P på Ω och ett stort heltal k och beräknar $Q = P + P + \cdots + P = kP$.
Om jag berättar P och Q för dig, kan du då säga vad k är?

Tillämpning: kryptering med elliptiska kurvor

Jag väljer en punkt P på Ω och ett stort heltal k och beräknar $Q = P + P + \cdots + P = kP$. Om jag berättar P och Q för dig, kan du då säga vad k är?

Detta är praktiskt sett omöjligt för stora k, även för en dator. Detta kan användas för att koda meddelanden.

Tillämpning: kryptering med elliptiska kurvor

Jag väljer en punkt P på Ω och ett stort heltal k och beräknar $Q = P + P + \cdots + P = kP$. Om jag berättar P och Q för dig, kan du då säga vad k är?

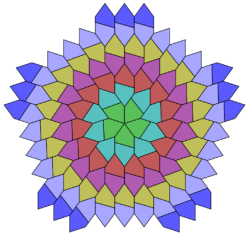
Detta är praktiskt sett omöjligt för stora k, även för en dator. Detta kan användas för att koda meddelanden.

I praktiken ersätter man $\mathbb{R}$ med $(\mathbb{Z}_p, +, \cdot)$ där p är ett stort primtal, kurvan är alltså $\{(x, y) \in (\mathbb{Z}_p)^2 \mid y^2 = x^3 - x + 1\} \cup \{\infty\}$

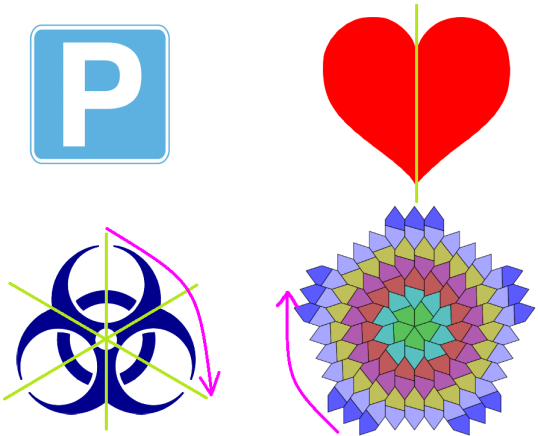
Del II

Symmetrier

Vilken av figurerna är mest symmetrisk?



Vilken av figurerna är mest symmetrisk?



Vad är en symmetri?

Informellt: En symmetri är förflyttning eller en omvandlig av ett objekt som lämnar objektet oförändrat.

Vad är en symmetri?

Informellt: En symmetri är förflyttning eller en omvandlig av ett objekt som lämnar objektet oförändrat.

Exempel från matematik och vetenskap:

- Matematik:Kombinatorik, geometri, algebra med mera
- Kemi: Symmetri i molekyler och kristaller
- Teoretisk fysik: Symmetrier i fysikens lagar
- Våglära: Symmetri i ljus- och ljud-vågor, signaler

Symmetrier bilder

Definition

En bild i planet kan beskrivas som en funktion $f : \mathbb{R}^2 \to F$ där F är en mängd färger.

Symmetrier bilder

Definition

En bild i planet kan beskrivas som en funktion $f : \mathbb{R}^2 \to F$ där F är en mängd färger.
En **symmetri** för bilden f kan definieras som en funktion $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ som uppfyller $f(\varphi(x)) = f(x)$ för alla $x \in \mathbb{R}^2$.

Symmetrier bilder

Definition

En bild i planet kan beskrivas som en funktion $f : \mathbb{R}^2 \to F$ där F är en mängd färger.
En **symmetri** för bilden f kan definieras som en funktion $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ som uppfyller $f(\varphi(x)) = f(x)$ för alla $x \in \mathbb{R}^2$.

Vi kräver också att φ är en **isometri**, det vill säga att φ är avståndsbevarande:
$|\varphi(x) - \varphi(y)| = |x - y|$.

Isometrier i planet

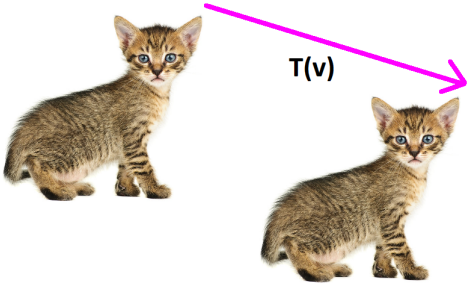
Sats

Det finns bara fyra typer av isometrier i planet:
translationer, **rotationer**, **speglingar**, och **glidspeglingar**.

Isometrier i planet

Sats

Det finns bara fyra typer av isometrier i planet:
translationer, **rotationer**, **speglingar**, och **glidspeglingar**.

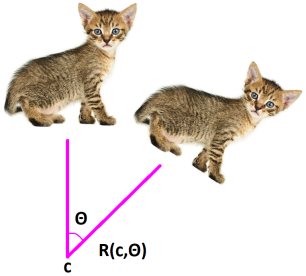


Translation längs vektorn v.

Isometrier i planet

Sats

Det finns bara fyra typer av isometrier i planet:
translationer, **rotationer**, **speglingar**, och **glidspeglingar**.

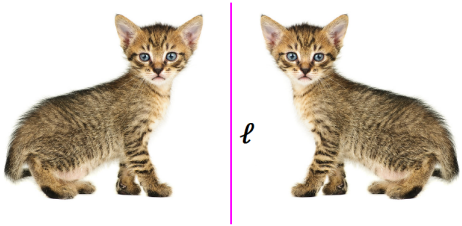


Rotation moturs vinkeln θ kring punkten c.

Isometrier i planet

Sats

Det finns bara fyra typer av isometrier i planet:
translationer, **rotationer**, **speglingar**, och **glidspeglingar**.

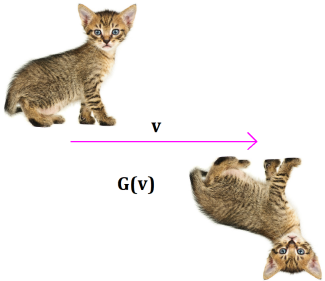


Spegling i linjen ℓ.

Isometrier i planet

Sats

Det finns bara fyra typer av isometrier i planet:
translationer, **rotationer**, **speglingar**, och **glidspeglingar**.



Glidspegling: Translation längs vektorn v följt av spegling i translationsriktningen.

Att kombinera isometrier

Sats

Sammansättningar av isometrier är isometrier.

Bevis: Låt φ och ψ vara isometrier, då är
$|(\psi \circ \varphi)(x) - (\psi \circ \varphi)(y)| = |\psi(\varphi(x)) - \psi(\varphi(y))| = |\varphi(x) - \varphi(y)| = |x - y|$.

Symmetrigrupper

Sats

Mängden symmetrier för en bild utgör en grupp under sammansättning.

Symmetrigrupper

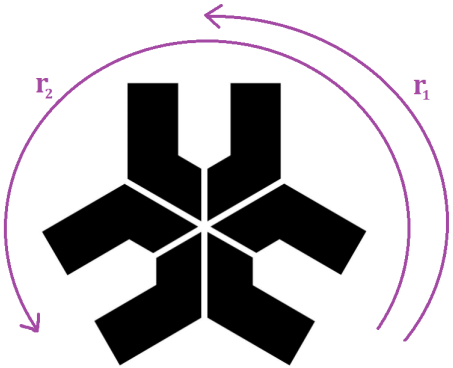
Sats

Mängden symmetrier för en bild utgör en grupp under sammansättning.

- Sammansättningen av två isometrier är en isometri
- Sammansättning är associativ: $(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1)$
- Identitetsavbildningen $e(x) = x$ är identitetselement
- Om f är en symmetri är också f^{-1} en symmetri

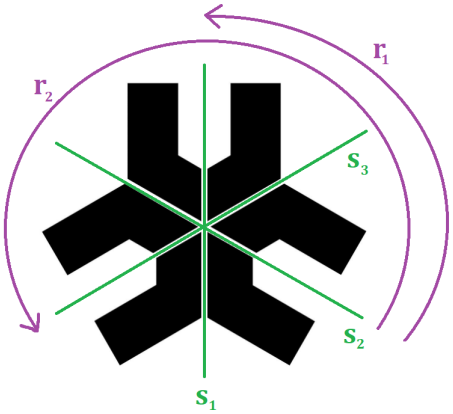
Gamla LiU-loggan

Gamla LiU-loggan



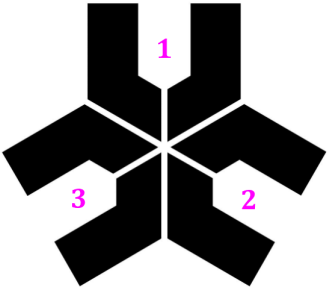
Figuren har 3 rotationssymmetrier: $\{e, r_1, r_2\}$

Gamla LiU-loggan



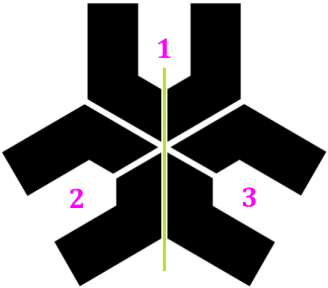
Figuren har 3 spegelsymmetrier: $\{s_1, s_2, s_3\}$

Gamla LiU-loggan



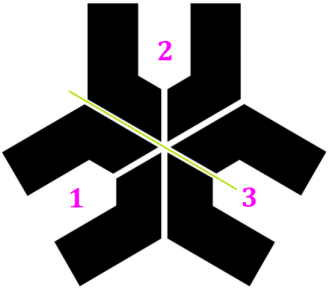
Vi namnger områden.

Gamla LiU-loggan



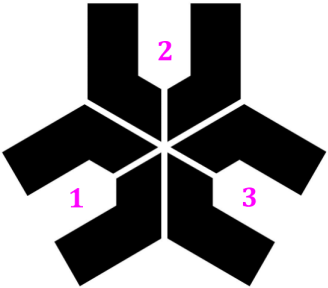
Vi speglar med $s_1 \ldots$

Gamla LiU-loggan



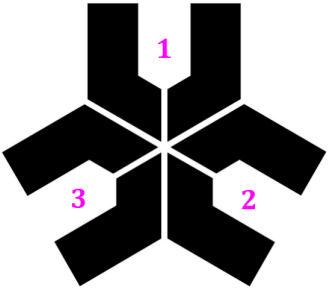
. . .och speglar sedan med s_2

Gamla LiU-loggan



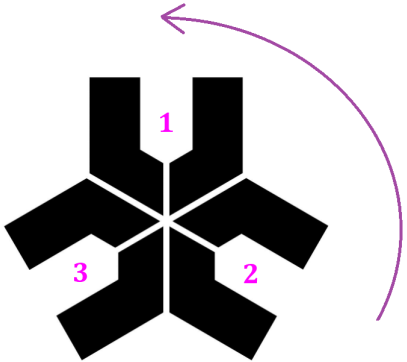
Resultatet efter bägge avbildningarna

Gamla LiU-loggan



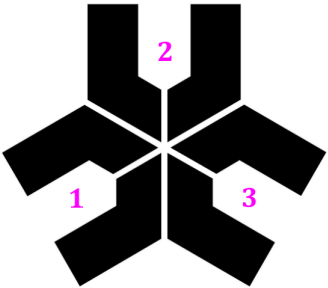
Ursprungsfiguren

Gamla LiU-loggan



Vi applicerar r_1

Gamla LiU-loggan



Slutsats: $s_2 \circ s_1 = r_1$

Multiplikationstabell för den dihedrala gruppen D_3

$\circ$	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_3	s_1	s_2
r_2	r_2	e	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r_2	r_1
s_2	s_2	s_3	s_1	r_1	e	r_2
s_3	s_3	s_1	s_2	r_2	r_1	e

Del III

Frismönster

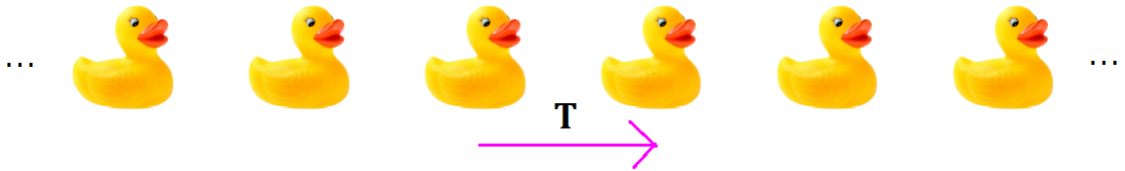
Ett frismönster

Mönster med translationssymmetri

...  ...

Vilka symmetrier har följande mönster?

Mönster med translationssymmetri



En translationssymmetri för varje heltal.

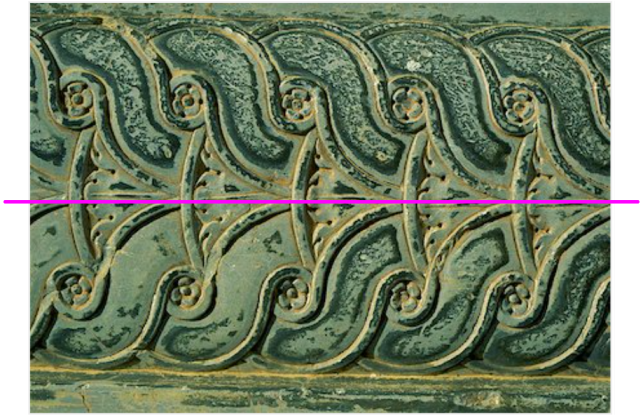
$$Sym(X) = \{ T^n \mid n \in \mathbb{Z} \} \simeq \mathbb{Z}$$

Hur många olika symmetrigrupper finns det för mönster som har translationssymmetri i en riktning?

Vilka symmetrier har mönstret?

Mönster i koppar

Vilka symmetrier har mönstret?



Spegling i en horisontell linje

Vilka symmetrier har mönstret?

Palacio de Velazquez, Parque de Retiro, Madrid, Spainien

Vilka symmetrier har mönstret?

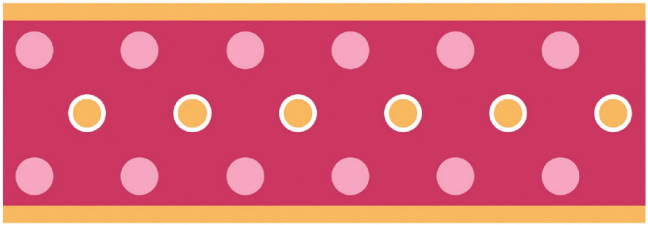
Vilka symmetrier har mönstret?

Spegelsymmetrier i verikala linjer

Vilka symmetrier har mönstret?

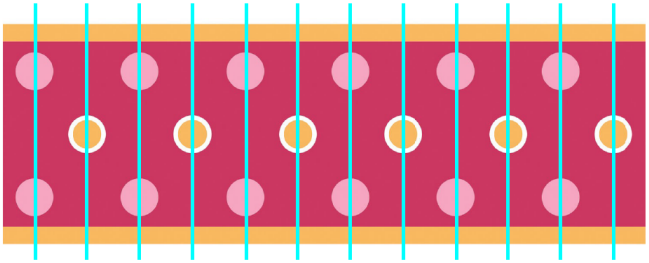
Ytterligare spegelsymmetrier av samma typ

Vilka symmetrier har mönstret?



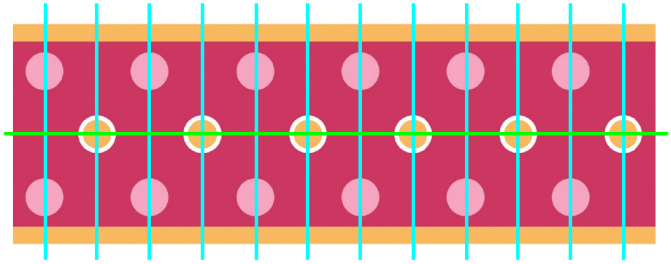
Tapetfris

Vilka symmetrier har mönstret?



Spegling i vertikala linjer

Vilka symmetrier har mönstret?

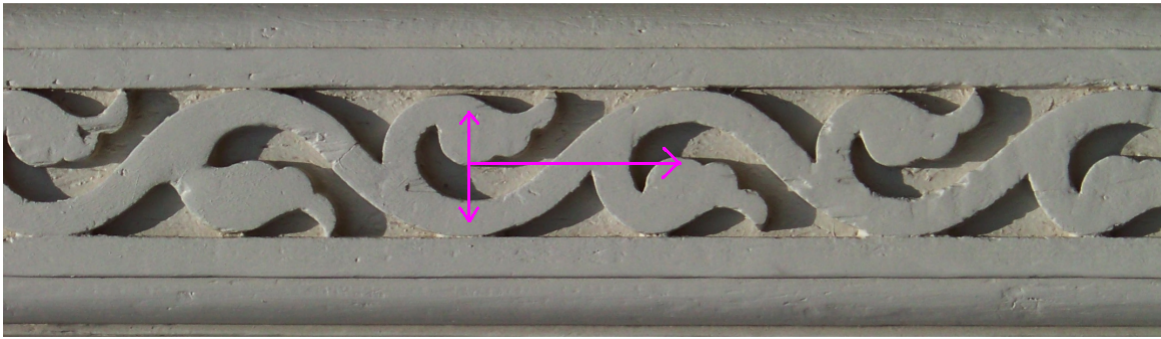


Spegling i en horisontell linje

Vilka symmetrier har mönstret?

Prydnadsmönster i sten

Vilka symmetrier har mönstret?

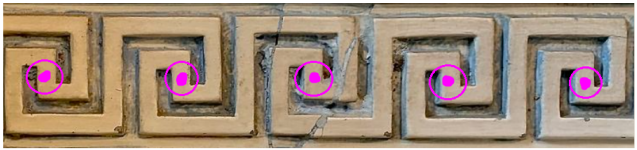


Glidreflektioner

Vilka symmetrier har mönstret?

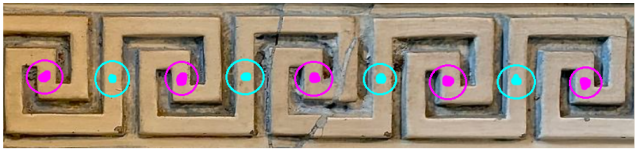
Grekiskt mönster, Dimitrie Sturdza House, Rumänien

Vilka symmetrier har mönstret?



Rotationssymmetrier

Vilka symmetrier har mönstret?

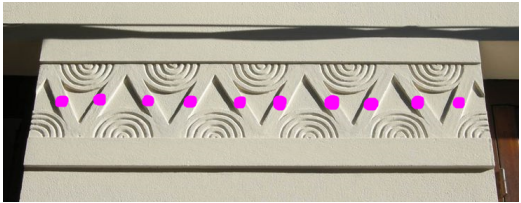


Ytterligare rotationssymmetrier

Vilka symmetrier har mönstret?

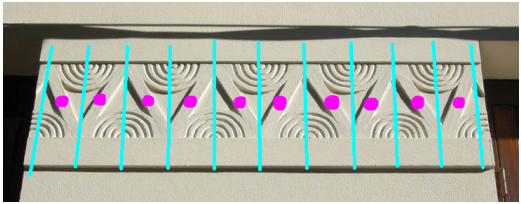
Mönster i sten, Uruguay

Vilka symmetrier har mönstret?



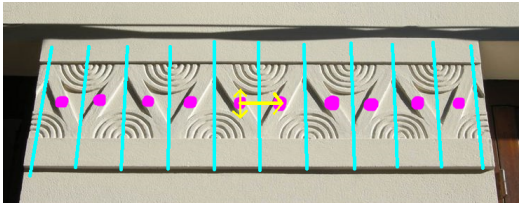
Rotationssymmetrier

Vilka symmetrier har mönstret?



Speglingar i vertikala linjer

Vilka symmetrier har mönstret?



Glidreflektioner

De sju möjliga Frisemönsterna

Namn	Symm.	Exempel
p1	T	
p11g	TG	
p1m1	TV	
p2	TR	
p2mg	TRVG	
p11m	THG	
p2mm	TRHVG	

Conways gångstilar

John Horton Conway

Namn	Symm.	Exempel
Hop	T	
step	TG	
sidle	TV	
spinning hop	TR	
spinning sidle	TRVG	
jump	THG	
spinning jump	TRHVG	

Del IV

Tapetgrupper

Tapetgrupperna

Tvådimensionella mönster med translationssymmetrier i två olika rikningar kan på liknande sätt kallas **tapetgrupper**.

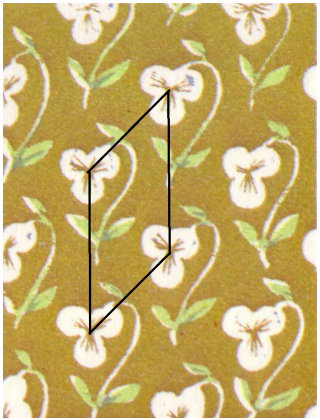
Två oberoende translationssymmetrier

Medeltida damaskering

Två oberoende translationssymmetrier

Två translationsriktningar

Två oberoende translationssymmetrier



Translationscell

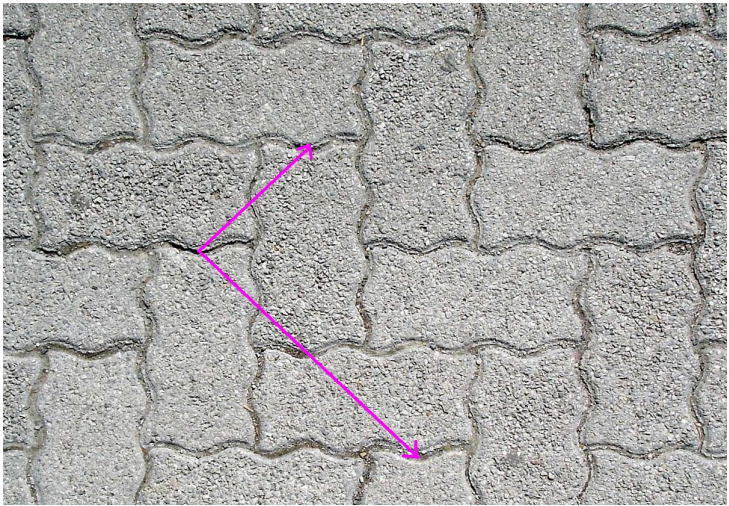
Två oberoende translationssymmetrier

Inga fler symmetrier

Fler symmetrier inom translationscellen

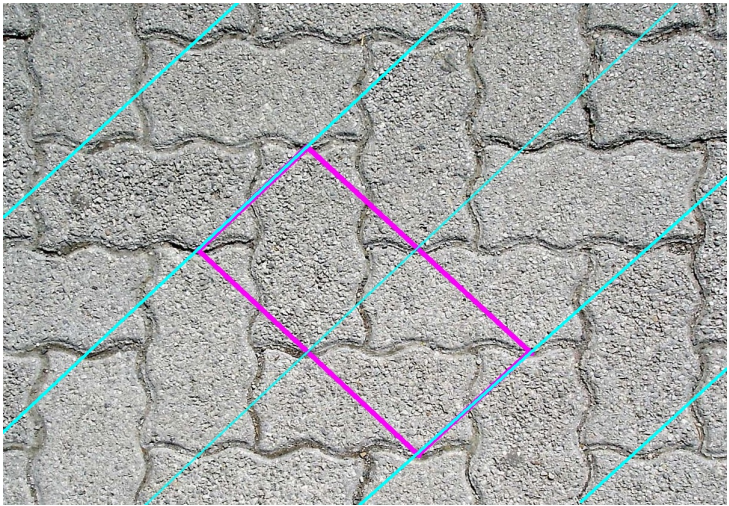
Trottoarmönster

Fler symmetrier inom translationscellen



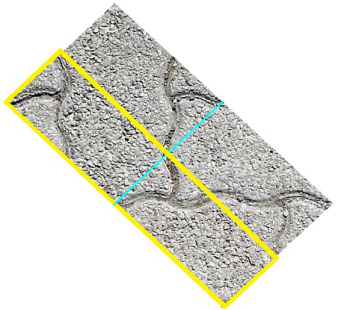
Två translationsriktningar

Fler symmetrier inom translationscellen



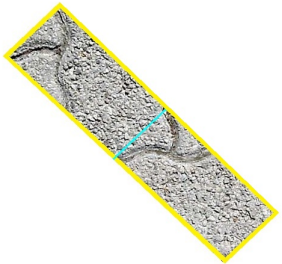
Glidreflektioner

Fler symmetrier inom translationscellen



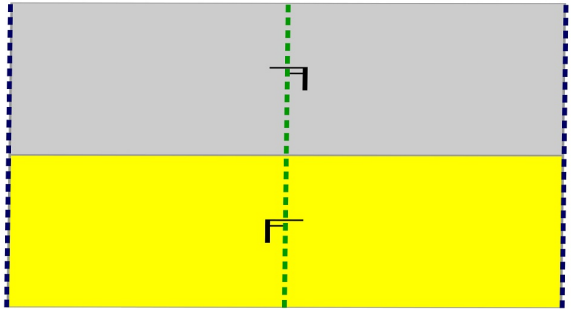
Translationscell

Fler symmetrier inom translationscellen



Fundamental cell

Fler symmetrier inom translationscellen



Symmetridiagram

Ännu ett exempel

M.C. Eschers fiskar

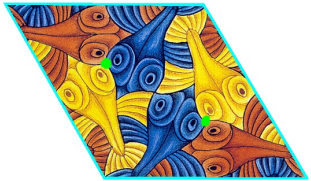
Ännu ett exempel

Sexfaldiga rotationer kring hörnen

Ännu ett exempel

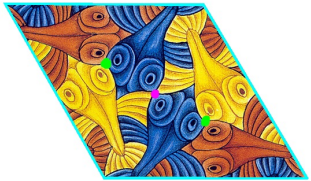
Translationscell

Ännu ett exempel



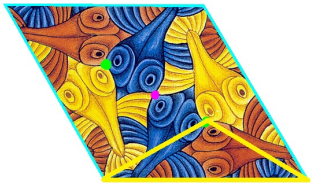
Trefaldiga rotationer inom cellen

Ännu ett exempel



En tvåfaldig rotation i cellens mitt

Ännu ett exempel

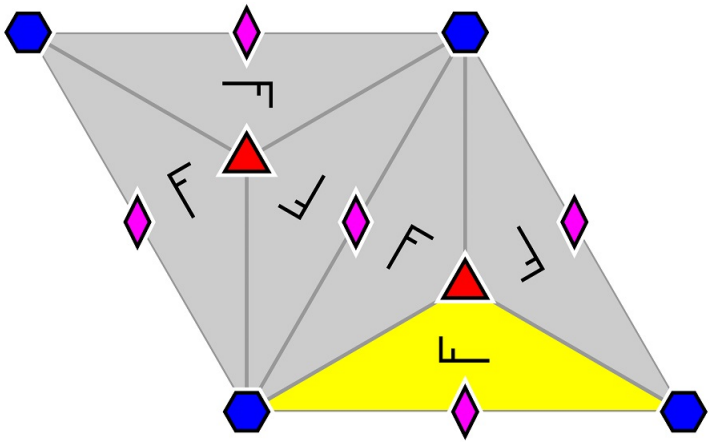


Fundamental cell

Ännu ett exempel

Fundamental cell

Ännu ett exempel



Symmetridiagram

De sjutton tapetgrupperna

Sats

Det finns exakt 17 olika tapetgrupper.

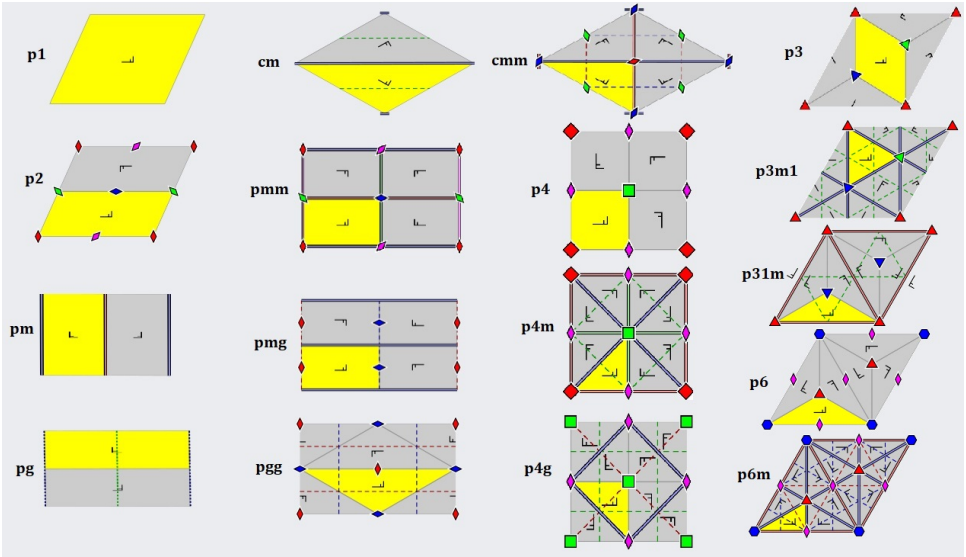
De sjutton tapetgrupperna

Sats

Det finns exakt 17 olika tapetgrupper.

Bevisades av Evgraf Fedorov 1891 och George Pólya 1924
(oberoende av varandra)

Klassifikation via symmetridiagram

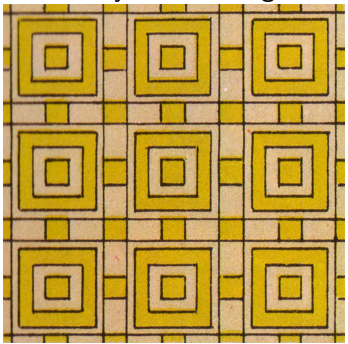


Vilken tapetgrupp tillhör min tapet?

<table>
<tr><th rowspan="2">Size of smallest rotation</th><th colspan="4">Has reflection?</th></tr>
<tr><td colspan="3">Yes</td><td>No</td></tr>
<tr><td>360° / 6</td><td colspan="3">p6m</td><td>p6</td></tr>
<tr><td rowspan="2">360° / 4</td><td colspan="3">Has mirrors at 45°?</td><td rowspan="2">p4</td></tr>
<tr><td colspan="2">Yes: p4m</td><td>No: p4g</td></tr>
<tr><td rowspan="2">360° / 3</td><td colspan="3">Has rot. centre off mirrors?</td><td rowspan="2">p3</td></tr>
<tr><td colspan="2">Yes: p31m</td><td>No: p3m1</td></tr>
<tr><td rowspan="4">360° / 2</td><td colspan="3">Has perpendicular reflections?</td><td rowspan="2">Has glide reflection?</td></tr>
<tr><td colspan="2">Yes</td><td>No</td></tr>
<tr><td colspan="2">Has rot. centre off mirrors?</td><td rowspan="2">pmg</td><td rowspan="2">Yes: pgg</td><td rowspan="2">No: p2</td></tr>
<tr><td>Yes: cmm</td><td>No: pmm</td></tr>
<tr><td rowspan="2">none</td><td colspan="3">Has glide axis off mirrors?</td><td colspan="2">Has glide reflection?</td></tr>
<tr><td colspan="2">Yes: cm</td><td>No: pm</td><td>Yes: pg</td><td>No: p1</td></tr>
</table>

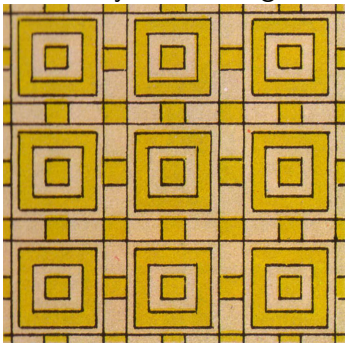
Vilken är mönstrets tapetgrupp?

Assyrisk målning



Vilken är mönstrets tapetgrupp?

Assyrisk målning

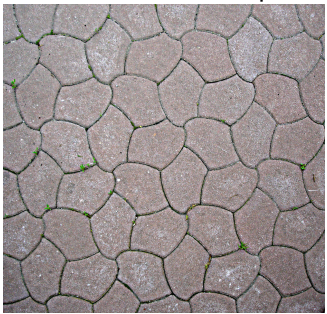


4-faldig rotationssymmetri, har reflektioner, har två spegelsymmetrilinjer med 45° vinkel.

p4m

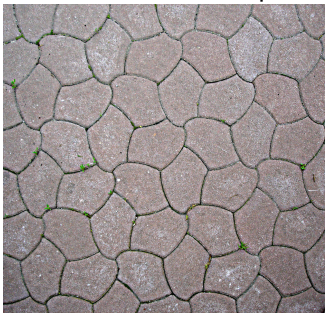
Vilken är mönstrets tapetgrupp?

Polsk trottoar, Zakopane



Vilken är mönstrets tapetgrupp?

Polsk trottoar, Zakopane

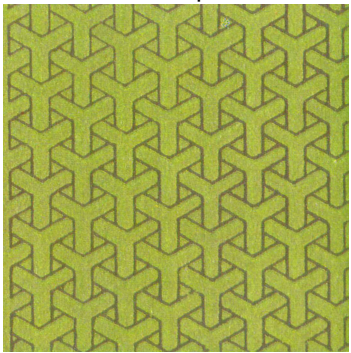


3-faldig rotationssymmetri, har inga reflektioner.

p3

Vilken är mönstrets tapetgrupp?

Kinesiskt porslin



Vilken är mönstrets tapetgrupp?

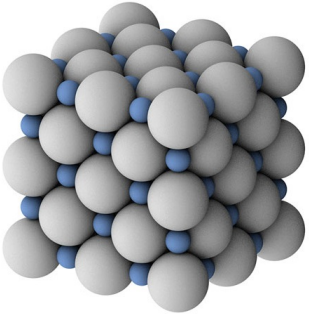
Kinesiskt porslin

3-faldig rotationssymmetri, har reflektioner, finns rotationscentrum som inte ligger på en spegellinje.

p31m

Tre dimensioner - Kristallografi

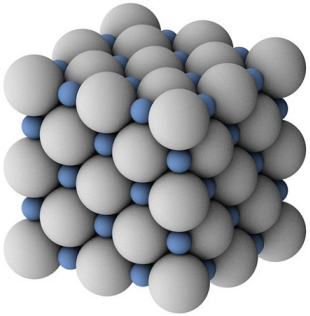
Fruktstapling



Saltkristall

Tre dimensioner - Kristallografi

Fruktstapling



Saltkristall

Sats

Det finns exakt **230** kristallografiska grupper - symmetrigrupper för tredimensionella mönster med tre oberoende translationsriktningar.

Ett par länkar

- https://en.wikipedia.org/wiki/Algebraic_structure
- https://en.wikipedia.org/wiki/Magma_(algebra)
- https://en.wikipedia.org/wiki/Euclidean_plane_isometry
- https://en.wikipedia.org/wiki/Frieze_group
- https://en.wikipedia.org/wiki/Wallpaper_group
- https://en.wikipedia.org/wiki/Symmetry_group

Ett par kurser

- TATA55 - Abstrakt algebra
- TATA49 - Geometri med tillämpningar

Tack!