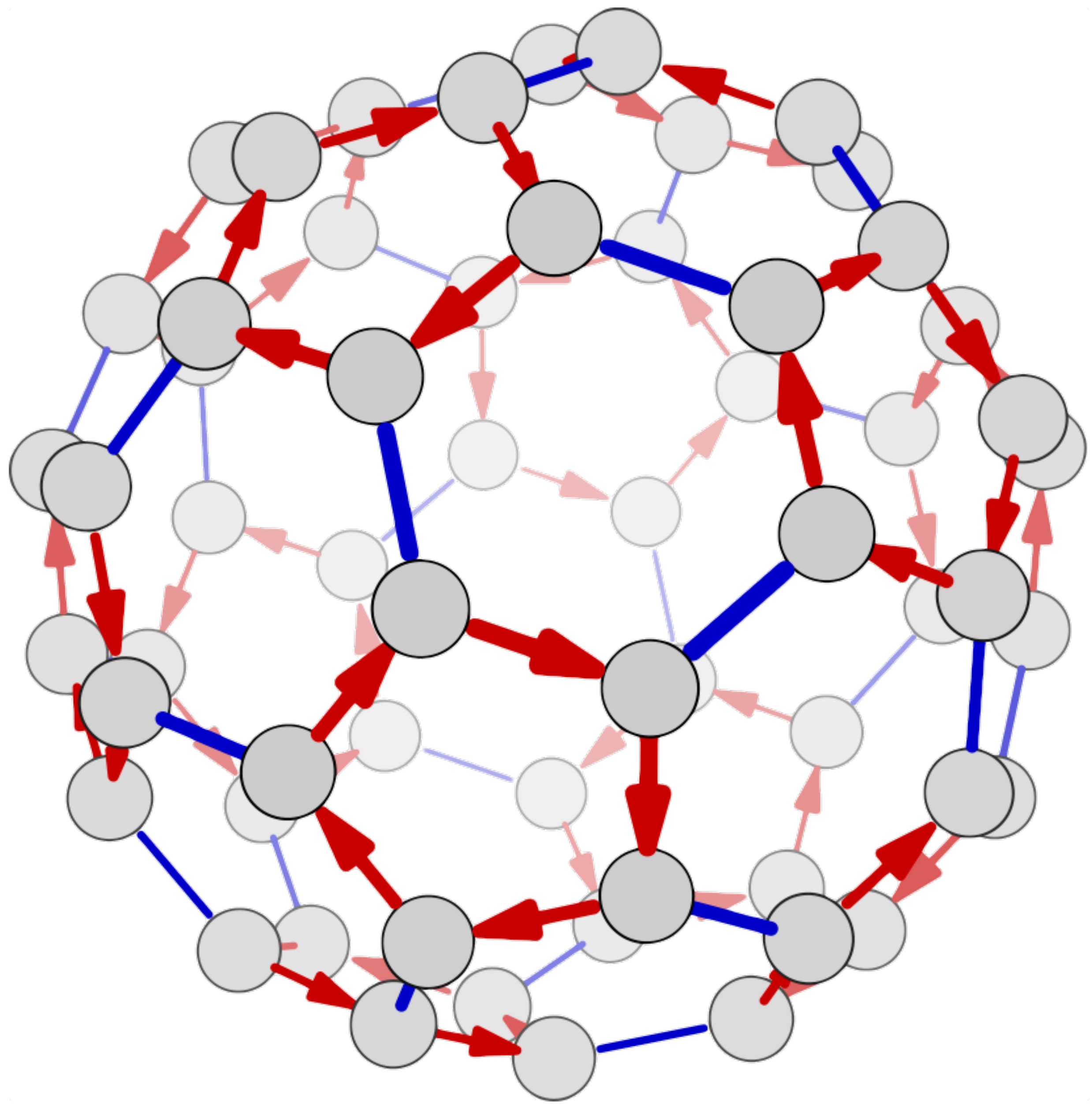
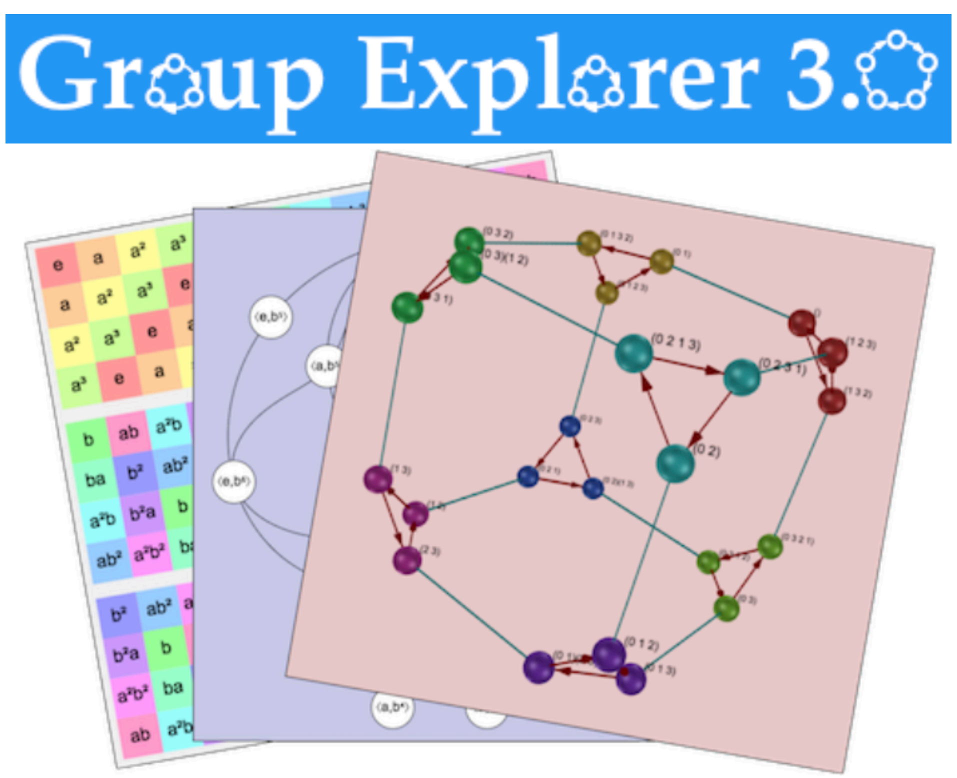
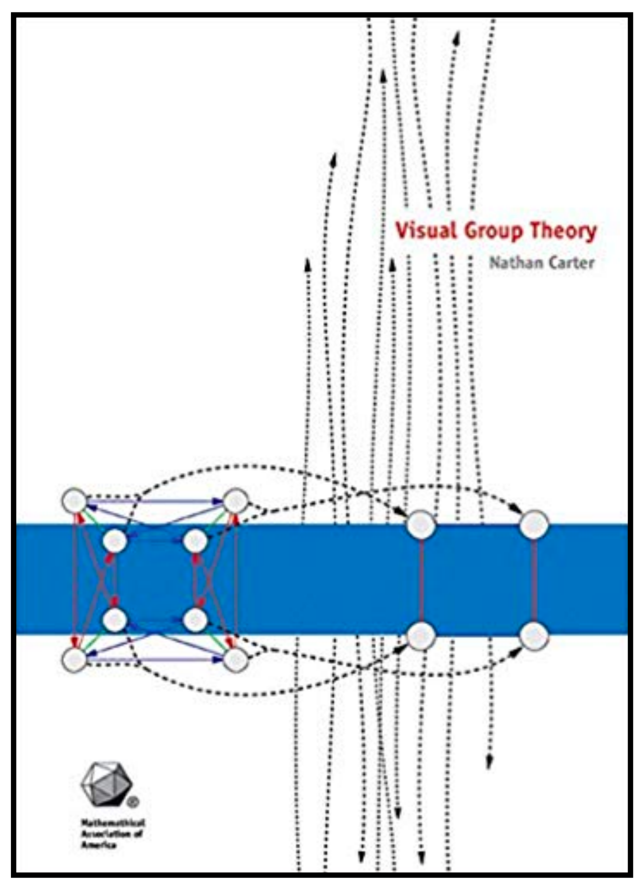
The Surprising Pedagogical Value and Versatility of Cayley Graphs



Nathan Carter, Bentley University

nathancarter.github.io





Five Definitions

1	A group is	**a set S**	(set)
2	with	**a binary operation * on S**	(magma)
3	that’s	**associative,**	(semigroup)
4	has	**an identity e,**	(monoid)
5	and has	**inverses for every element.**	(group)

Five Definitions

1	A group is **a set S**	(set)
2	with **a binary operation * on S**	(magma)
3	that's **associative,**	(semigroup)
4	has **an identity e,**	(monoid)
5	and has **inverses for every element.**	(group)

Five Definitions

1	A group is **a set S**	(set)
2	with **a binary operation * on S**	(magma)
3	that's **associative,**	(semigroup)
4	has **an identity e,**	(monoid)
5	and has **inverses for every element.**	(group)

	0	1	2	3	⋯	n-1
0						
1						
2						
3						
⋮						
n-1						

	0	1	2	3	$\cdots$	n-1
0	6	3	0	4	$\cdots$	0
1	4	2	2	3	$\cdots$	0
2	3	1	0	7	$\cdots$	7
3	7	7	7	4	$\cdots$	3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
n-1	0	1	1	1	$\cdots$	5

	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0

	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0

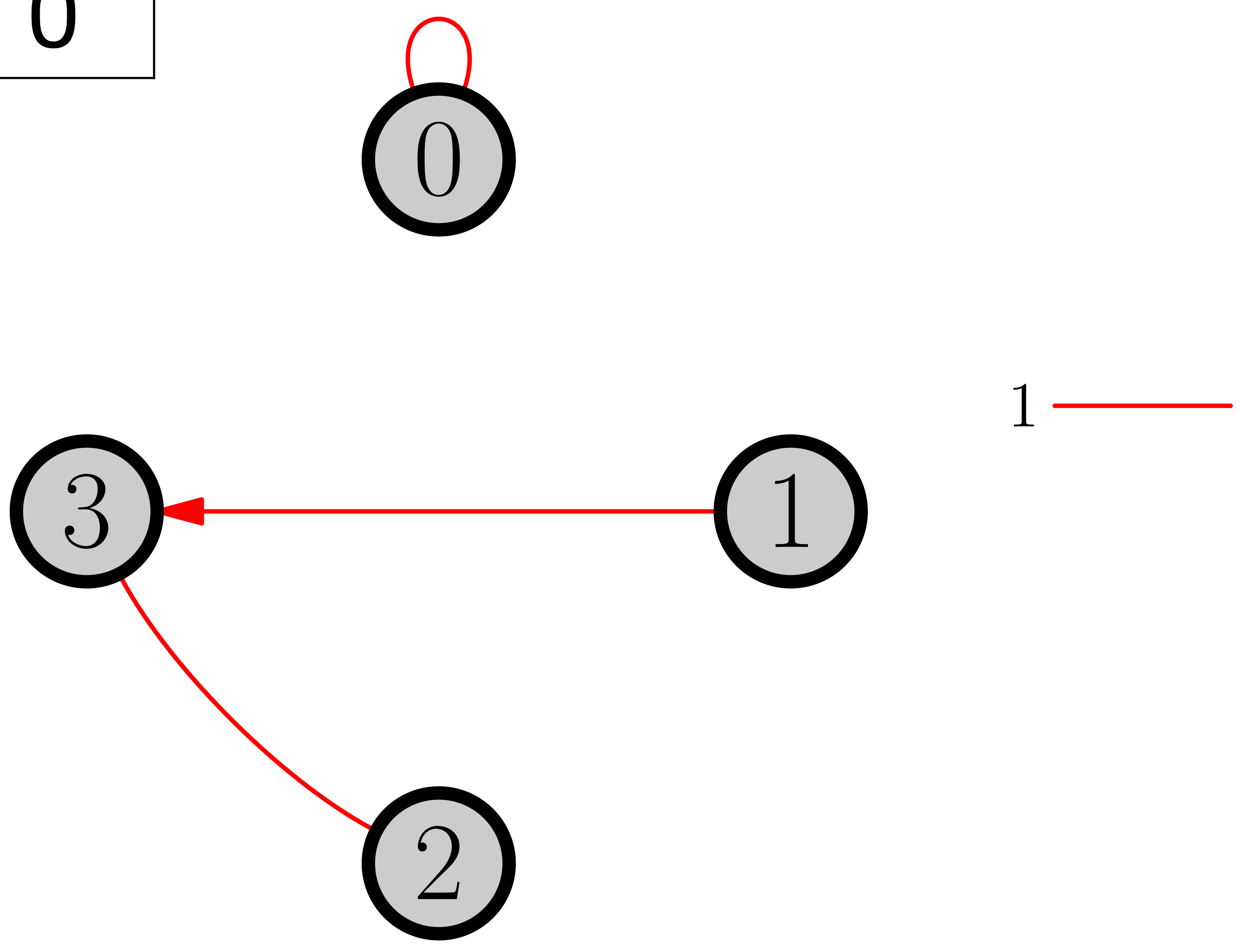
	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0

	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0

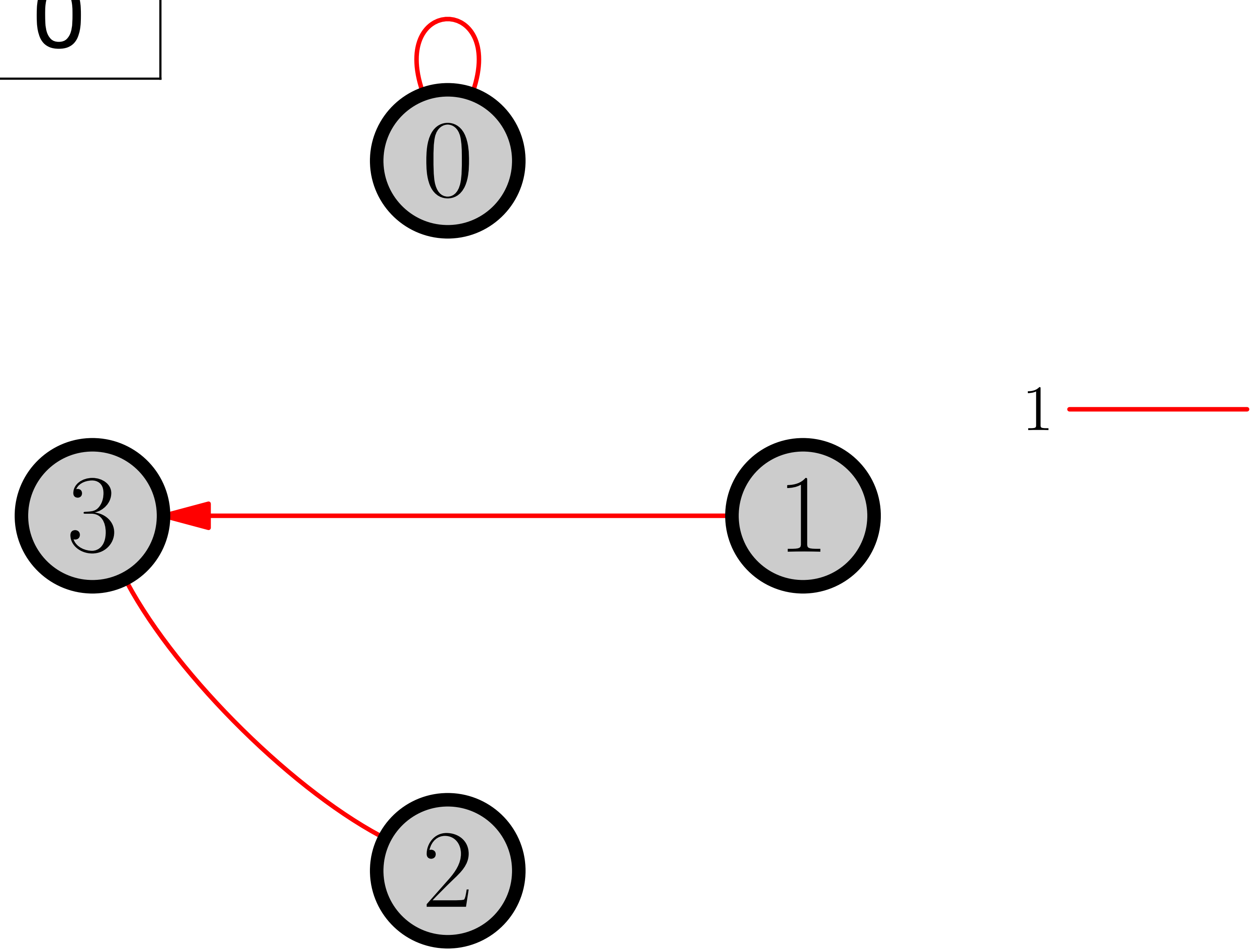
	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0

	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0

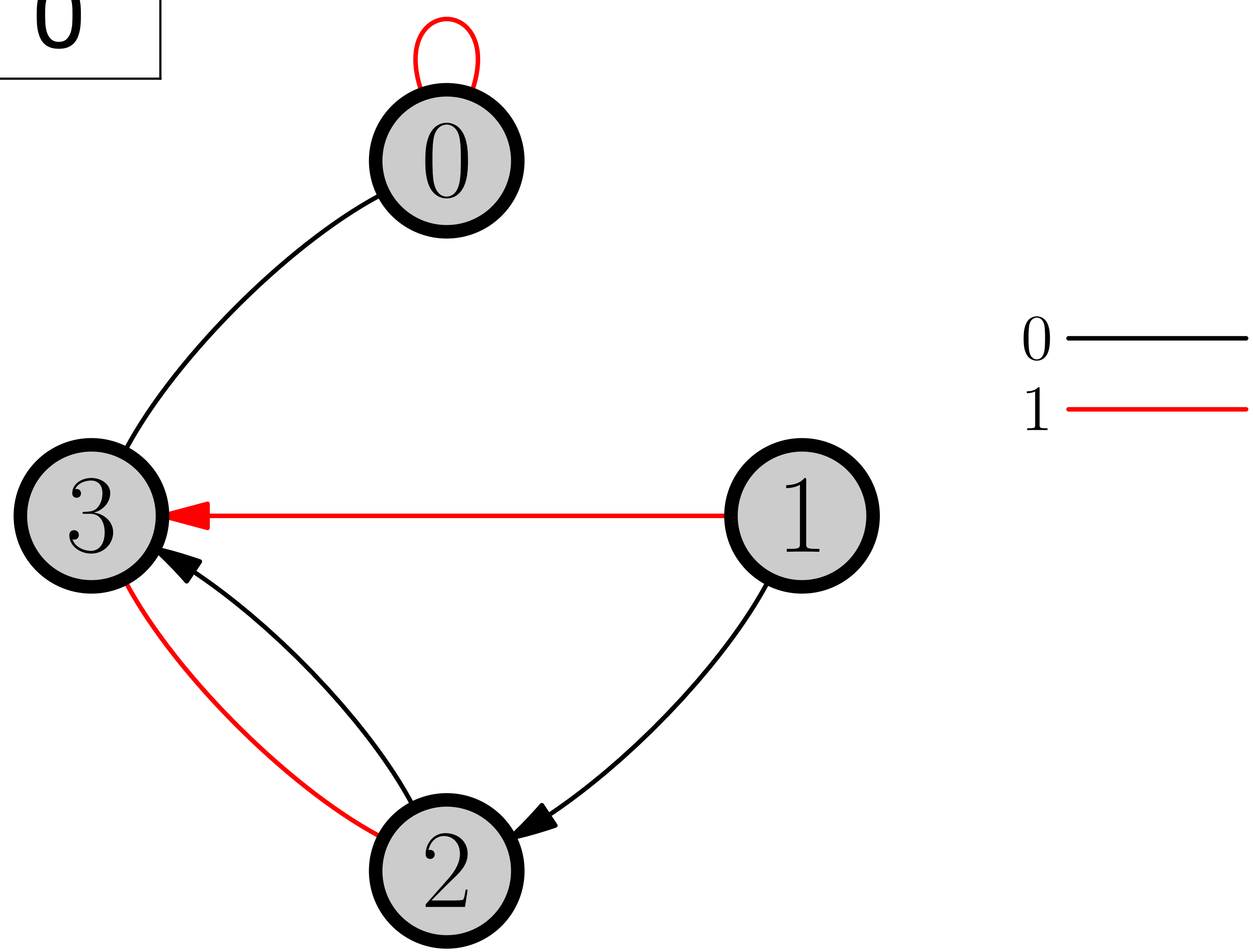
	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0



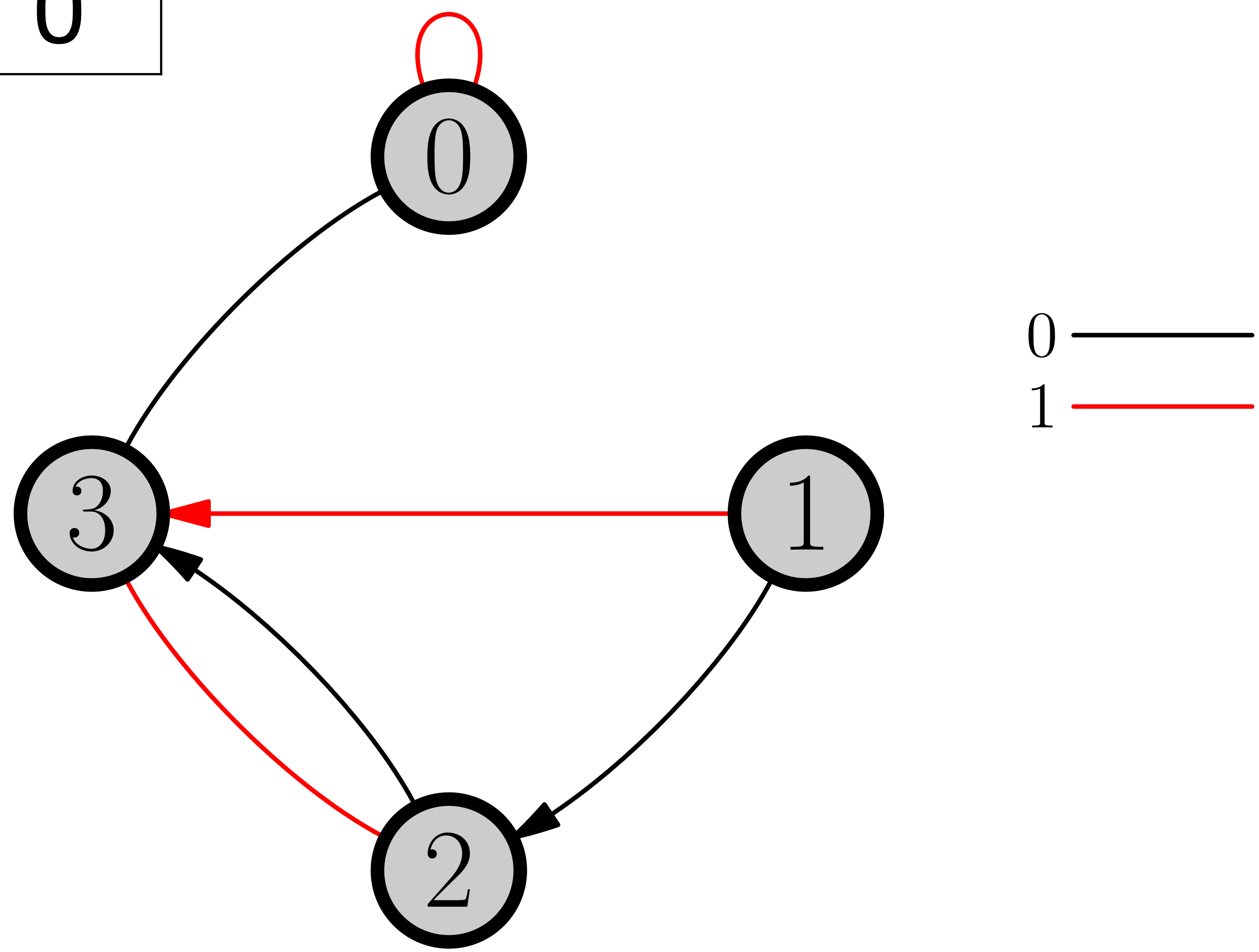
	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0



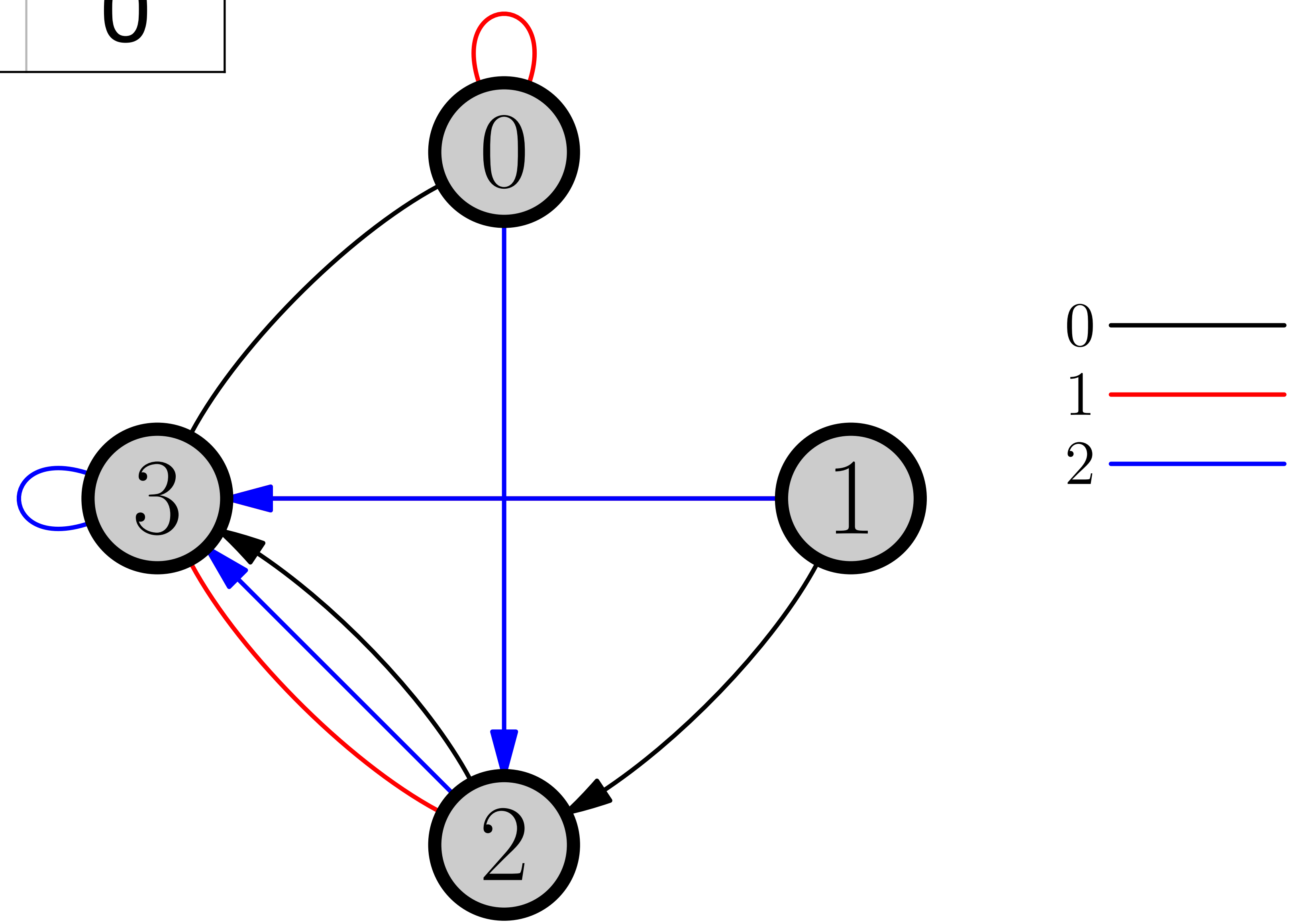
	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0



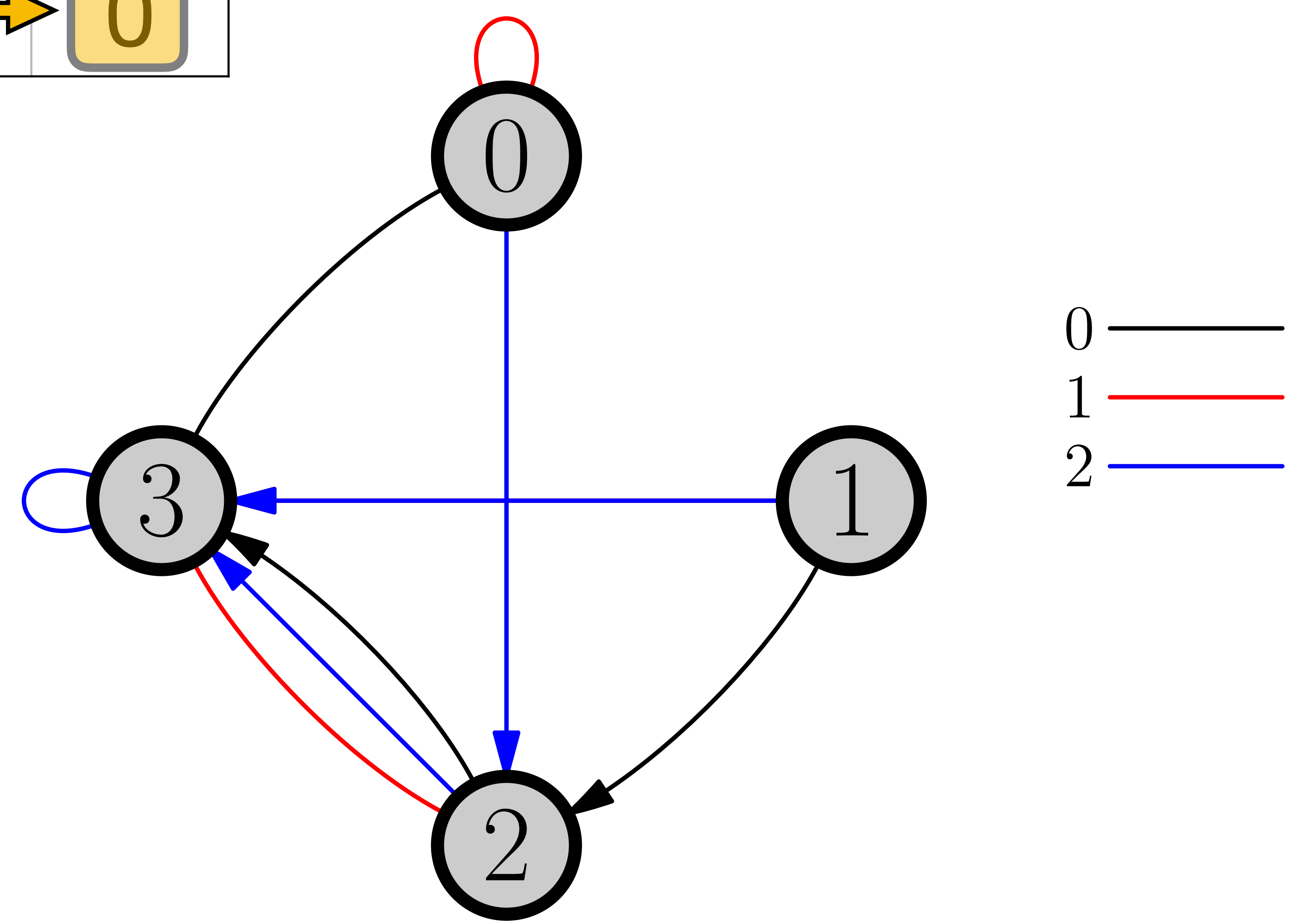
	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0



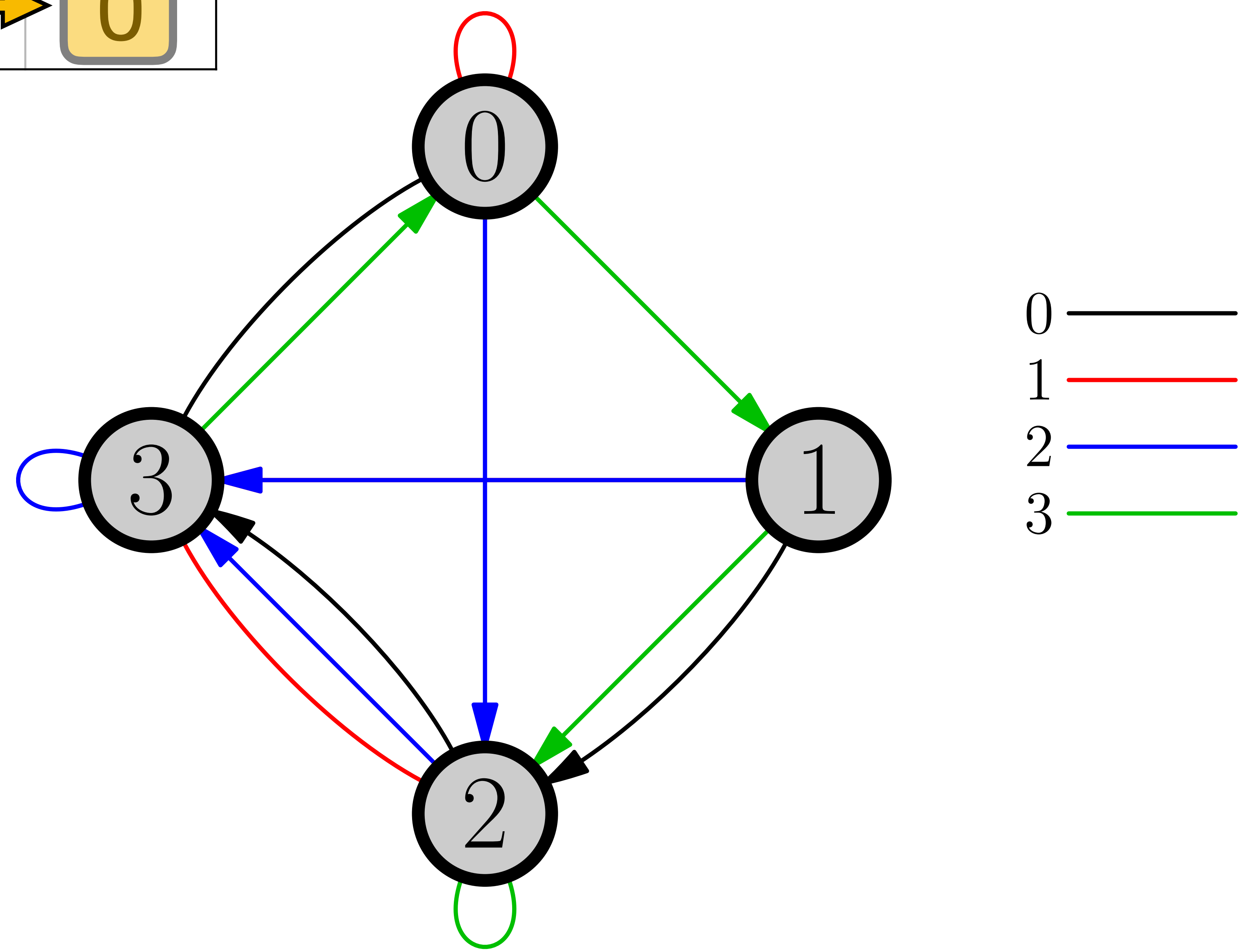
	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0



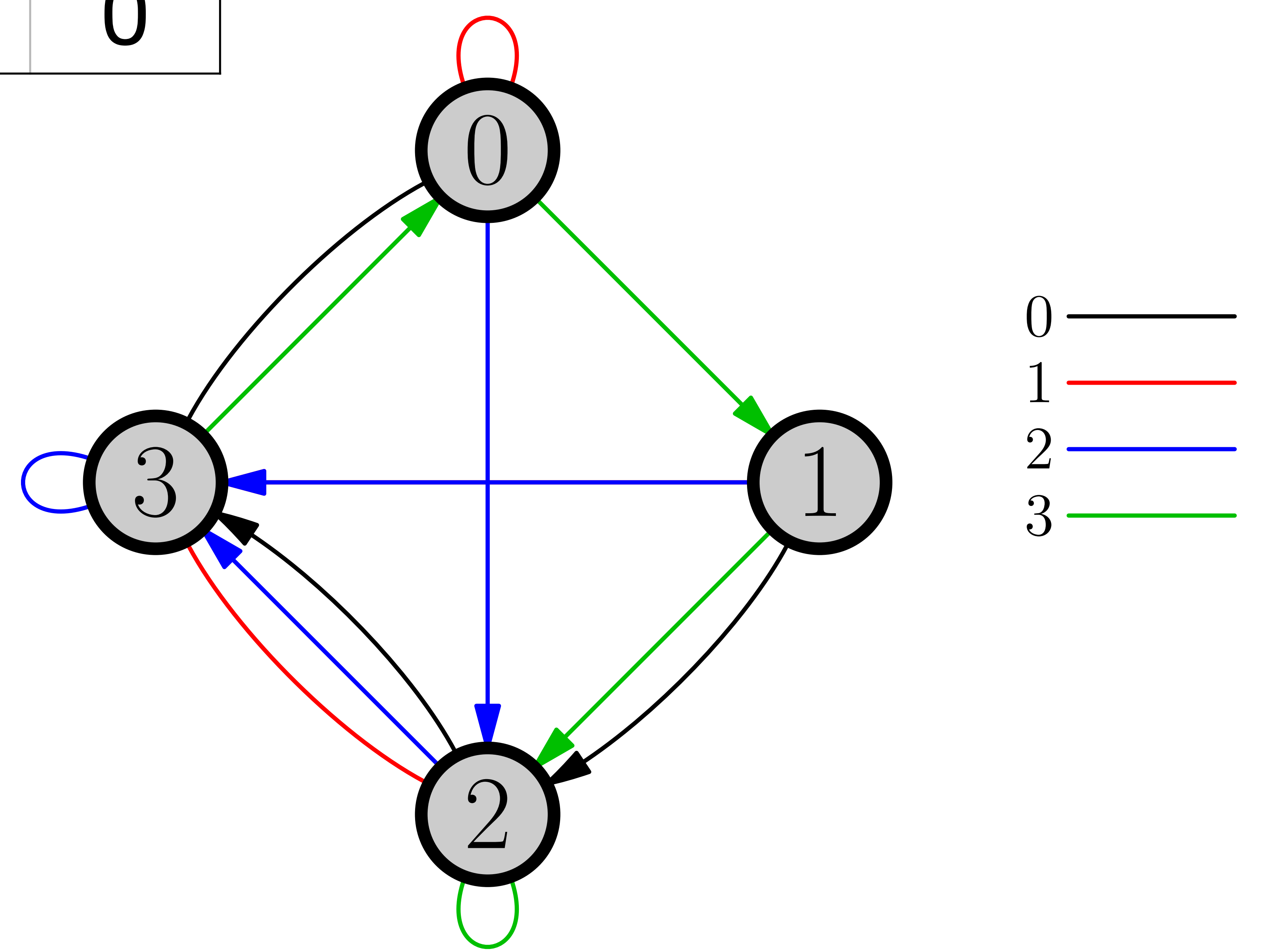
	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0



	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0



	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0



Generators

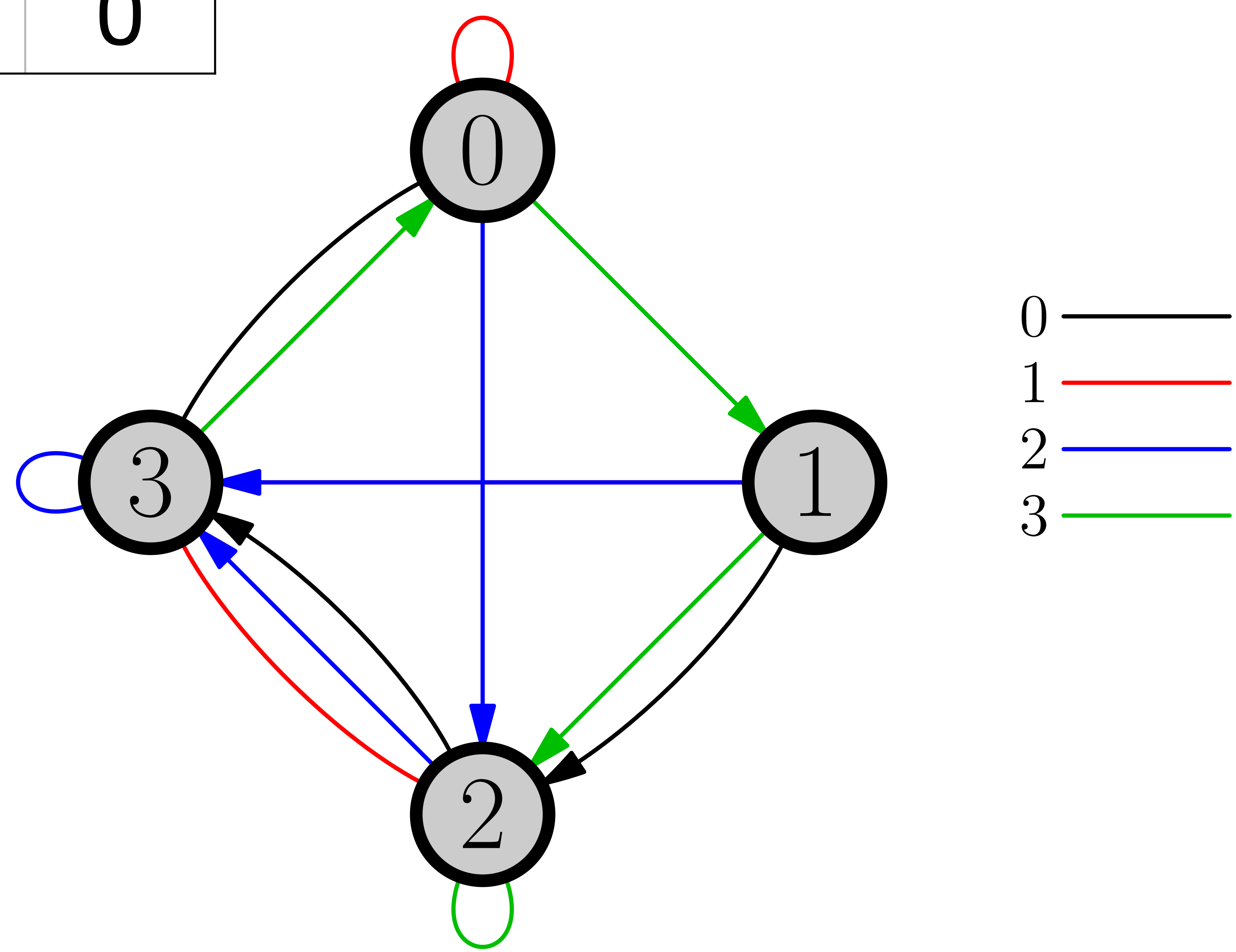
To compute: $x * y$

Use generators: $y = g_1 * \cdots * g_k$

Then compute: $x * (g_1 * \cdots * g_k)$

Problem: $(\cdots(x * g_1) * \cdots) * g_k)$

	0	1	2	3
0	3	0	2	1
1	2	3	3	2
2	3	3	3	2
3	0	2	3	0



Five Definitions

1	A group is **a set S**	(set)
2	with **a binary operation * on S**	(magma)
3	that's **associative,**	(semigroup)
4	has **an identity e,**	(monoid)
5	and has **inverses for every element.**	(group)

Five Definitions

1	A group is **a set S**	(set)
2	with **a binary operation * on S**	(magma)
3	that’s **associative,**	(semigroup)
4	has **an identity e,**	(monoid)
5	and has **inverses for every element.**	(group)

Generators

To compute: $x * y$

Use generators: $y = g_1 * \cdots * g_k$

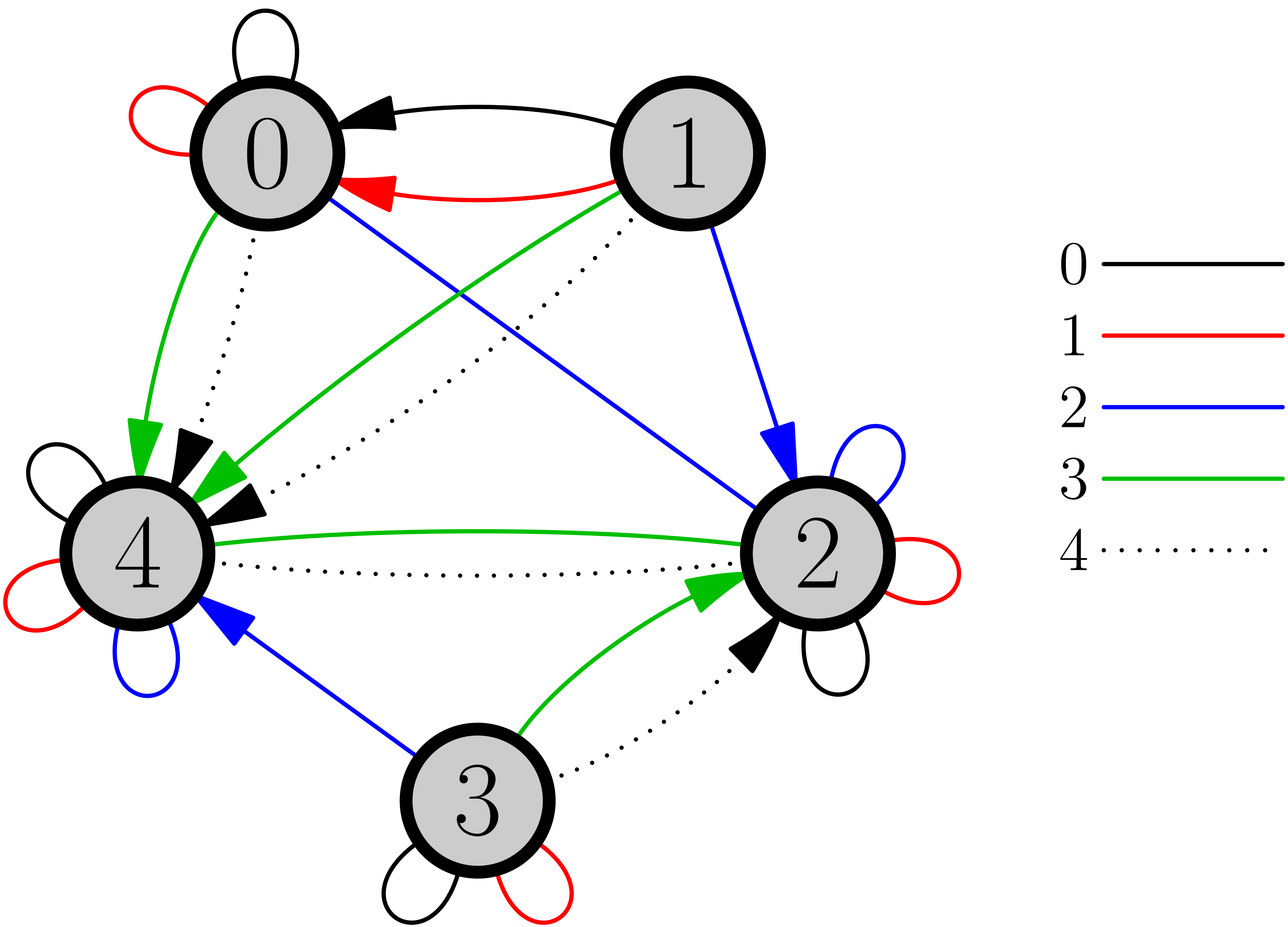
Then compute: $x * (g_1 * \cdots * g_k)$

Problem: $(\cdots(x * g_1) * \cdots) * g_k)$

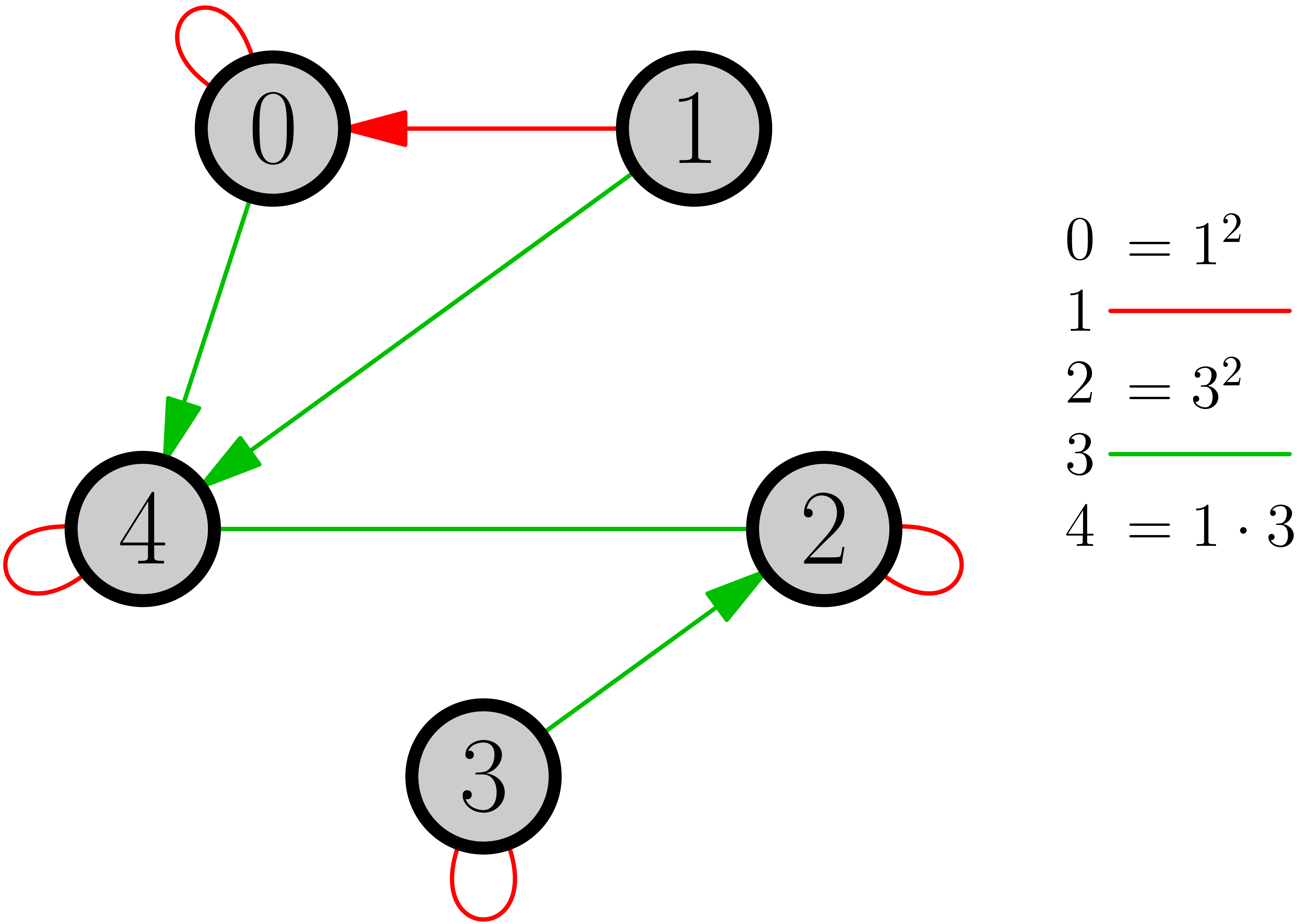
Generators

To compute:	$x * y$
Use generators:	$y = g_1 * \cdots * g_k$
Then compute:	$x * (g_1 * \cdots * g_k)$
~~Problem:~~	$(\cdots(x * g_1) * \cdots) * g_k)$

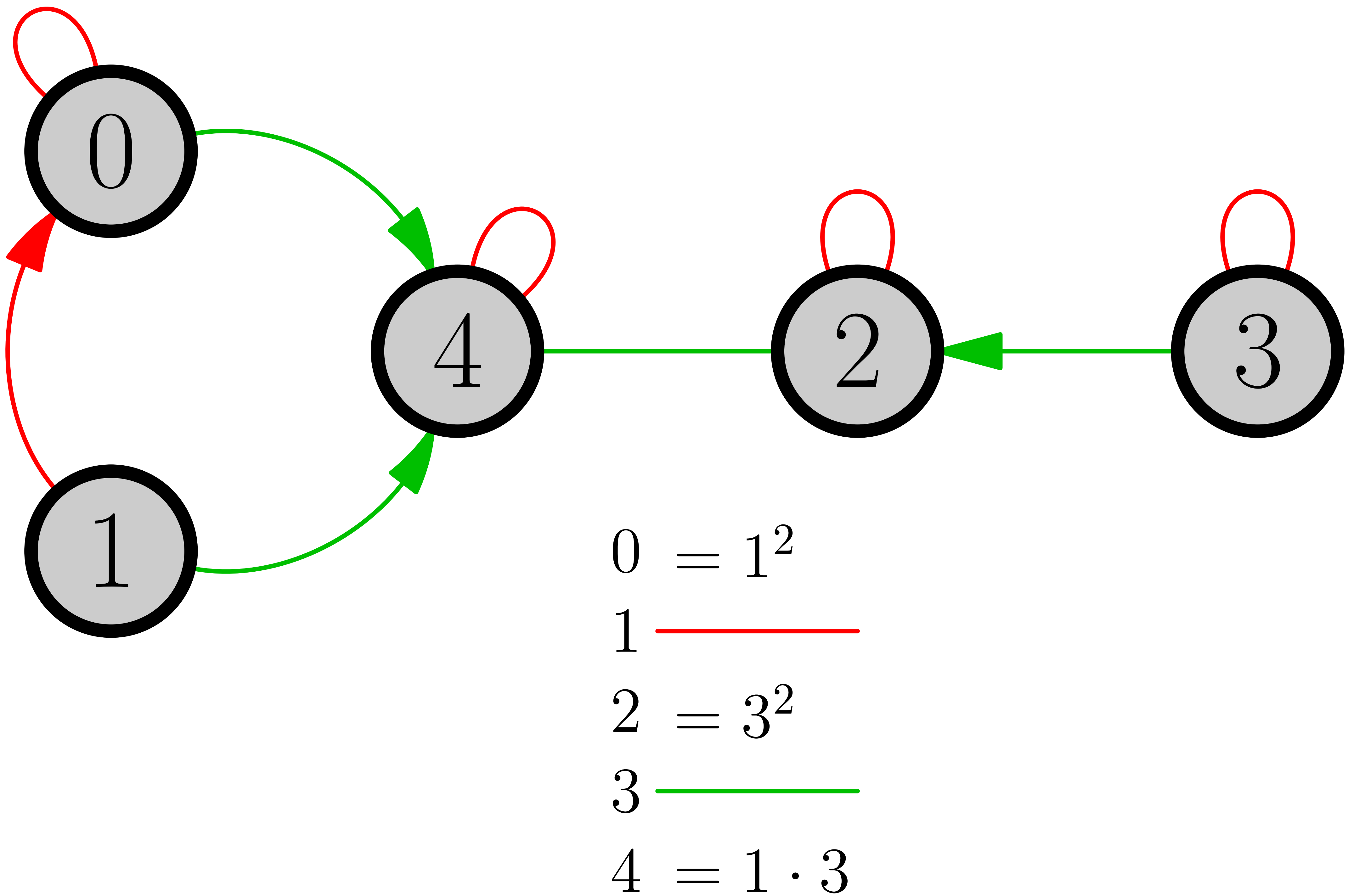
	0	1	2	3	4
0	0	0	2	4	4
1	0	0	2	4	4
2	2	2	2	4	4
3	3	3	4	2	2
4	4	4	4	2	2

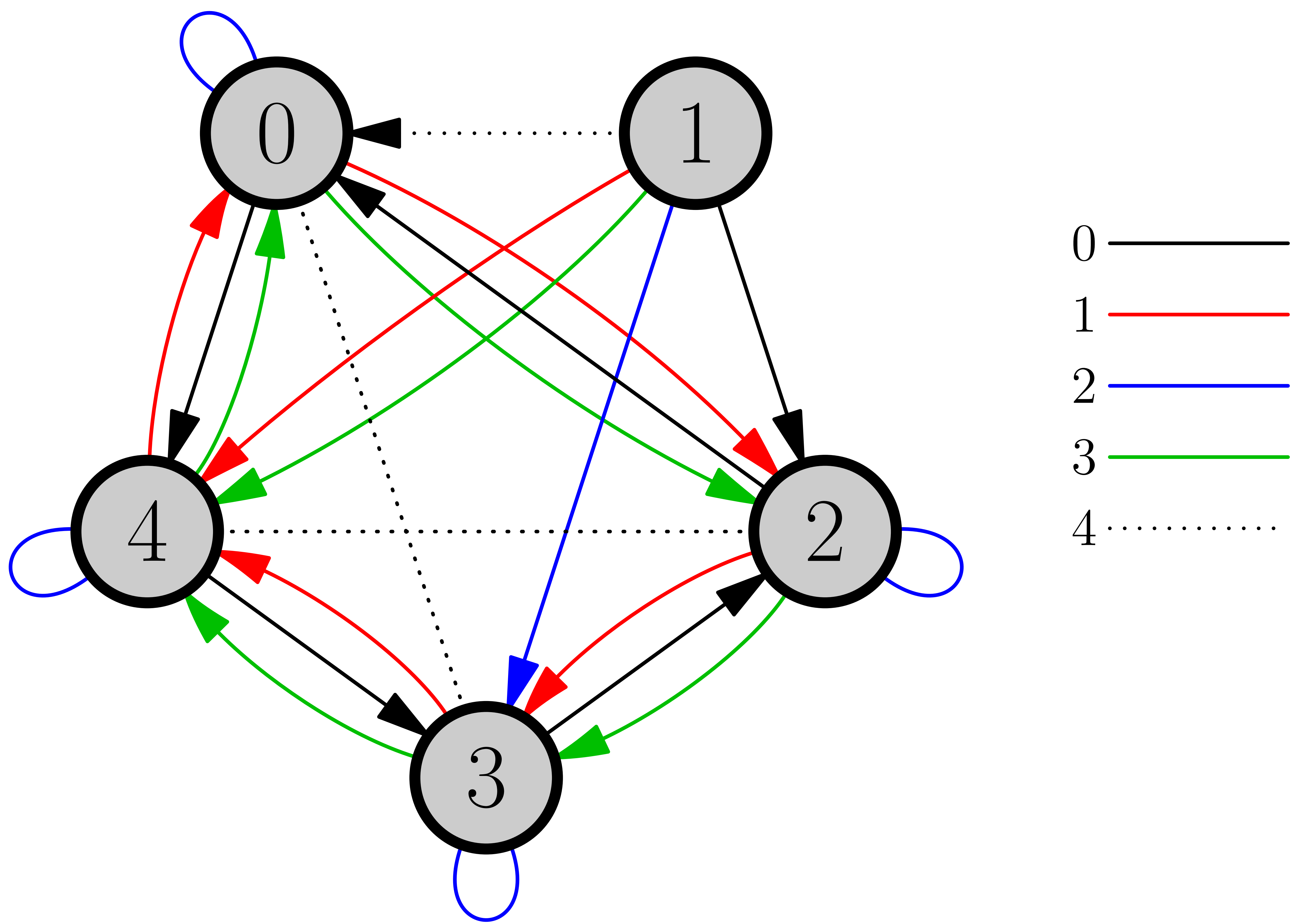


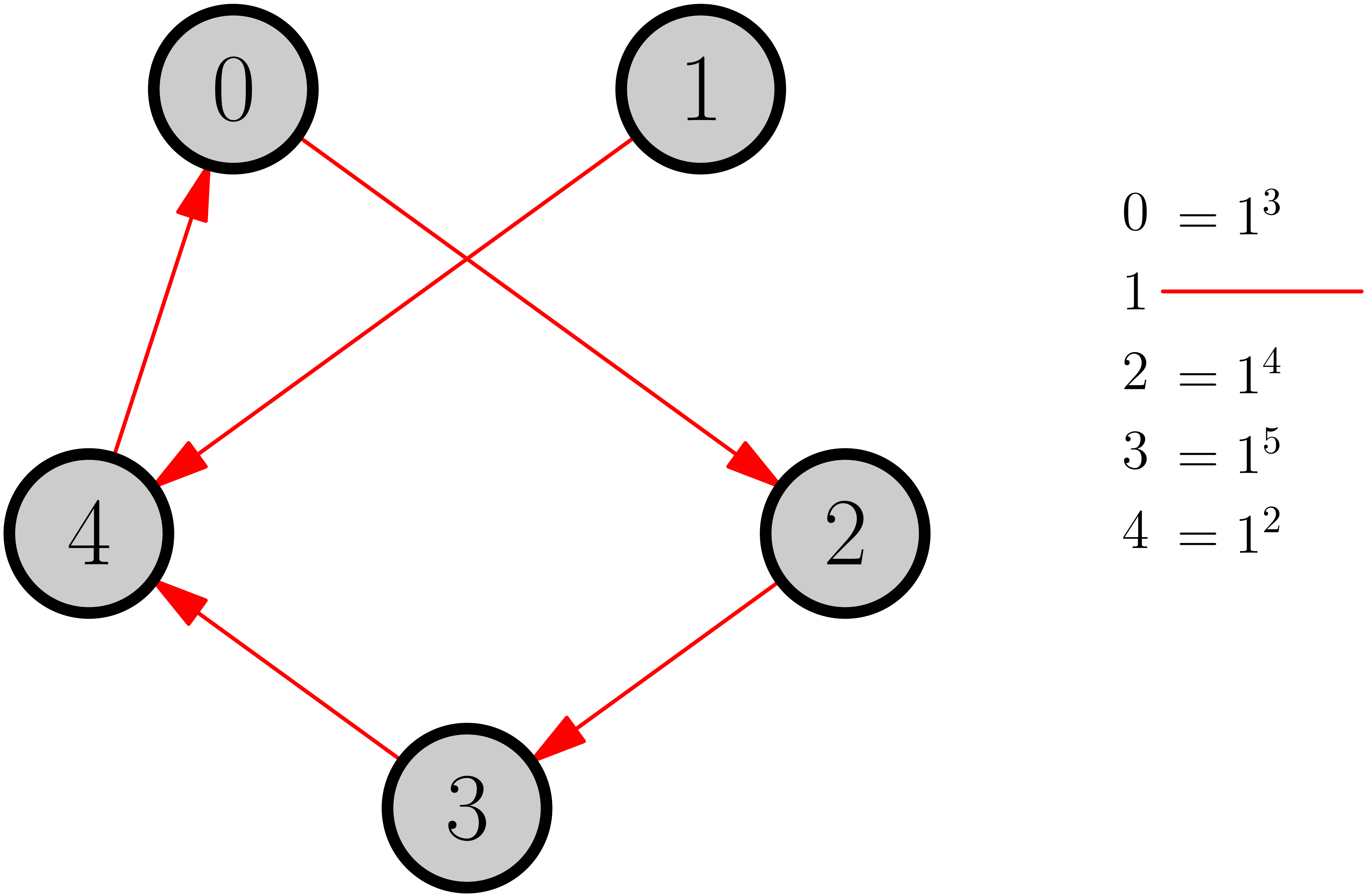
0
1
2
3
4
0
1
2
3
4

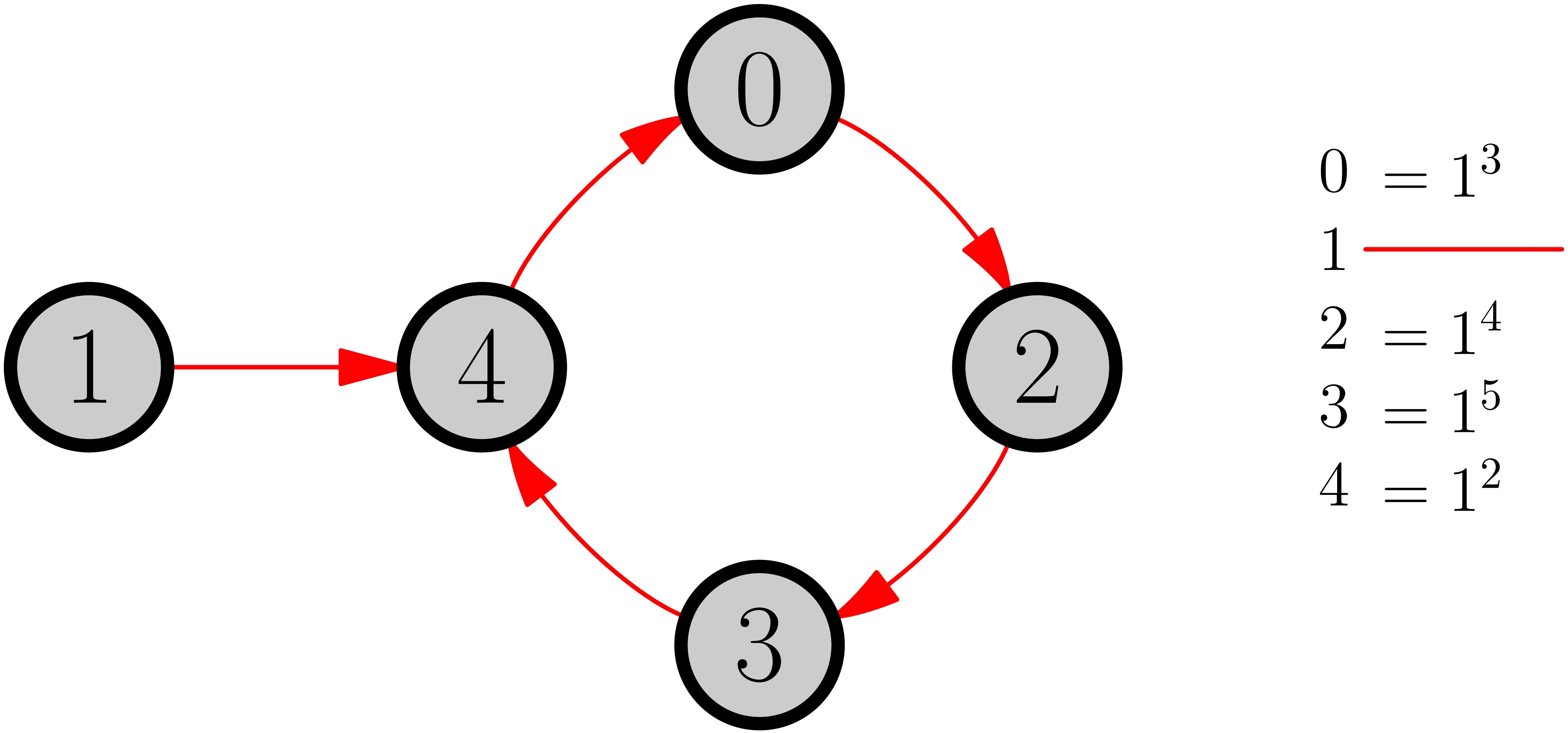


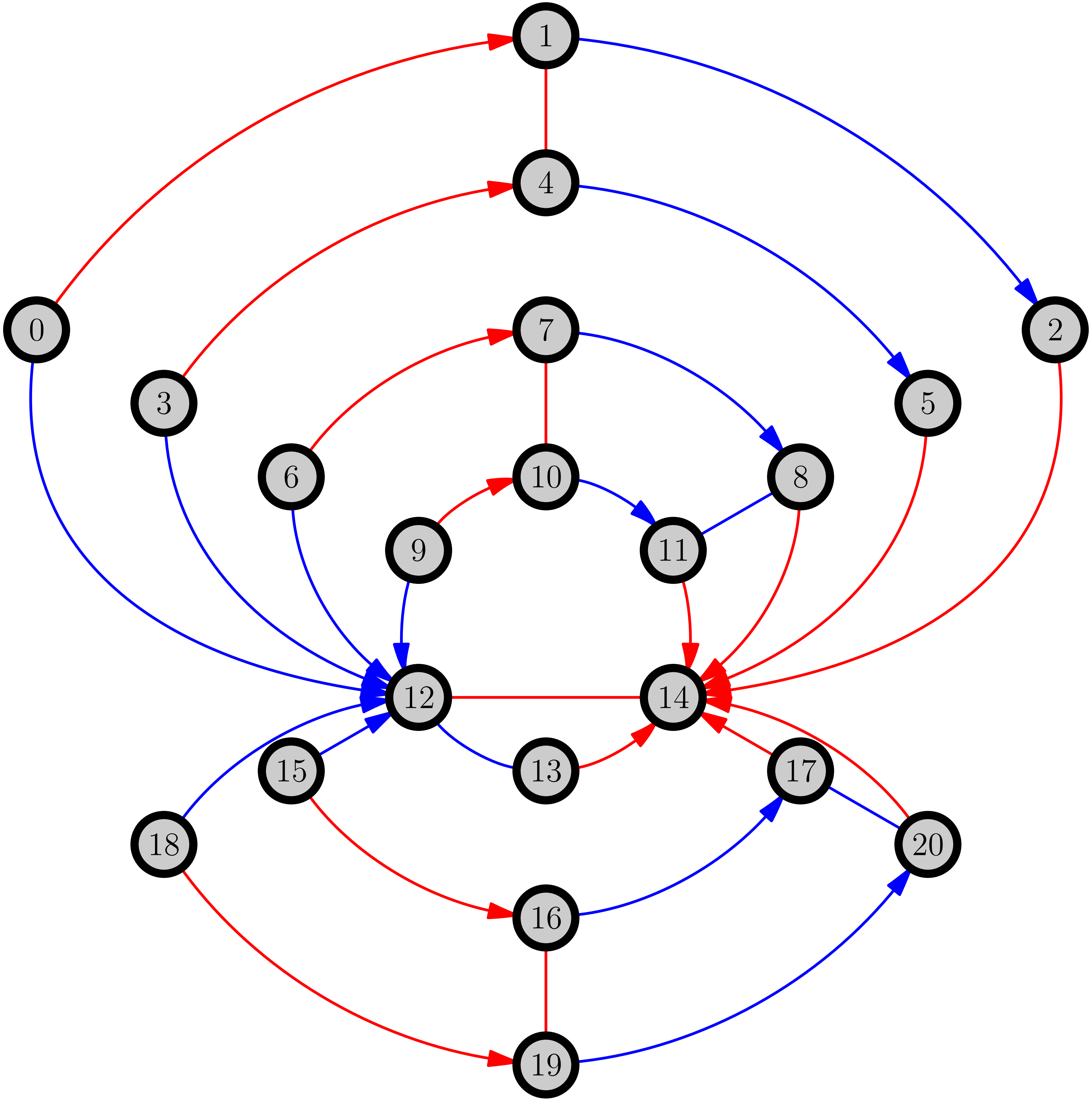
0
1
2
3
4
$0 = 1^2$
1
$2 = 3^2$
3
$4 = 1 \cdot 3$


0
1
2
3
4
$0 = 1^2$
1
$2 = 3^2$
3
$4 = 1 \cdot 3$

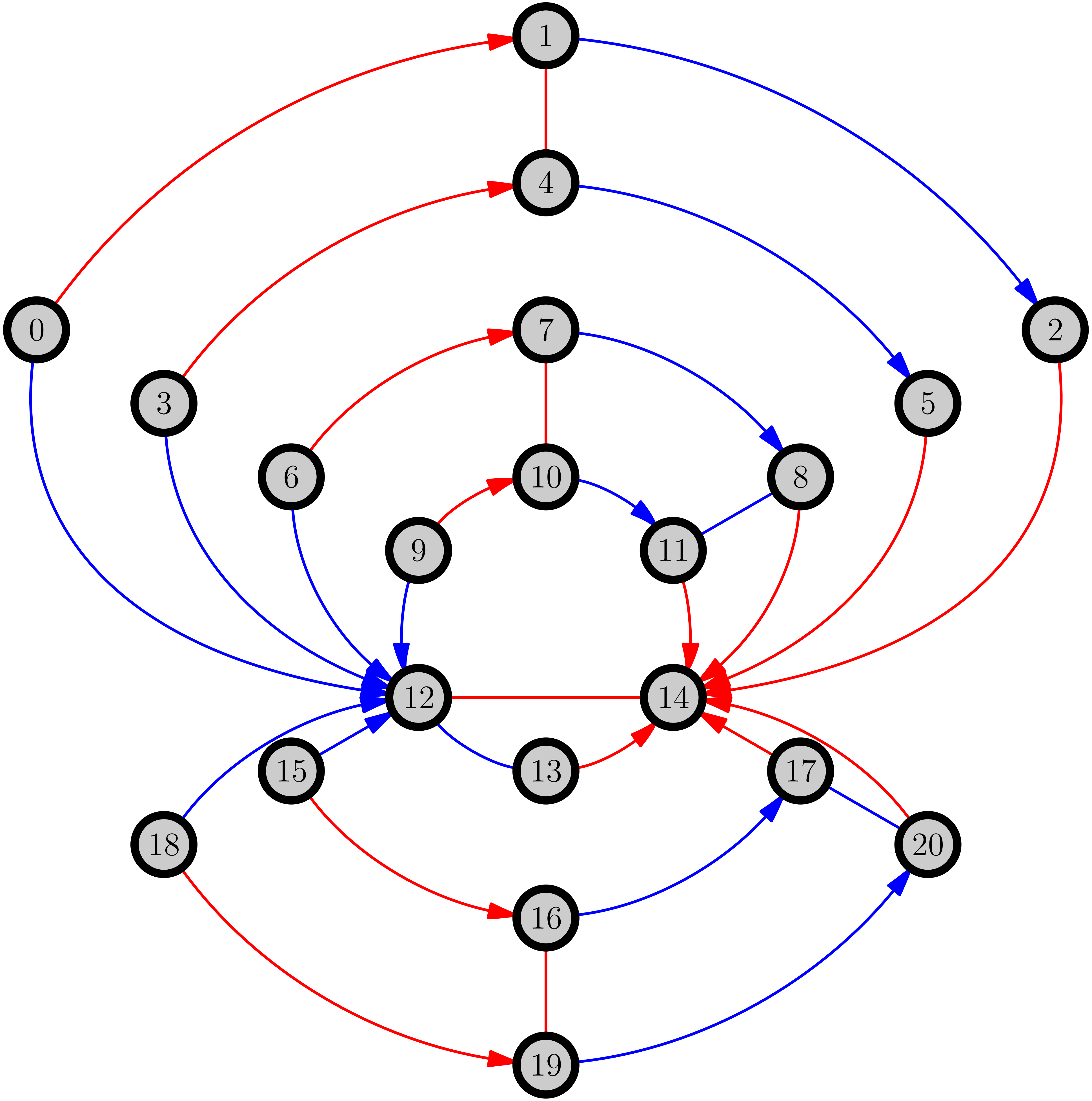

0
1
2
3
4
0
1
2
3
4

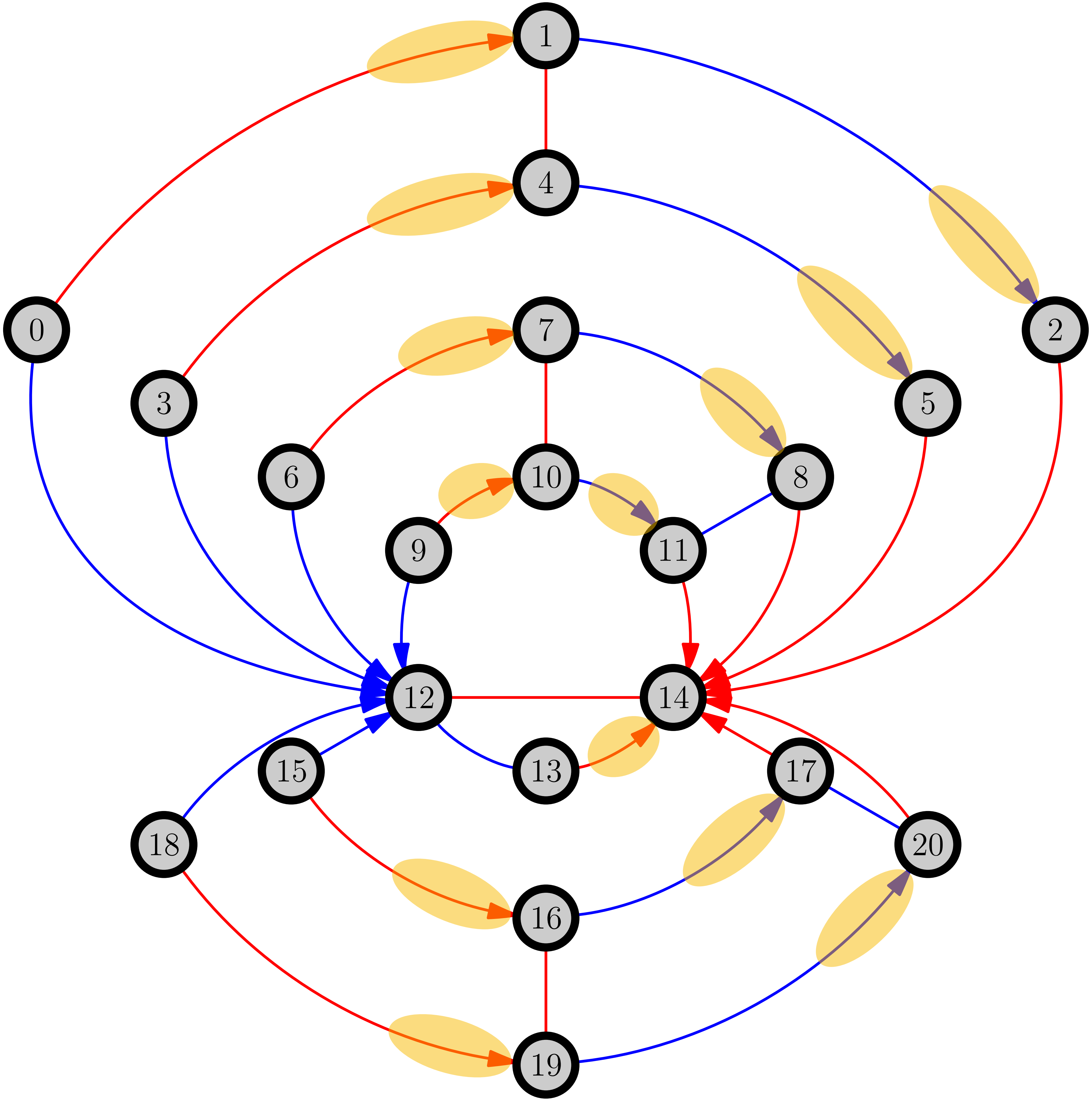

0
1
4
2
3
0 = 1³
1
2 = 1⁴
3 = 1⁵
4 = 1²

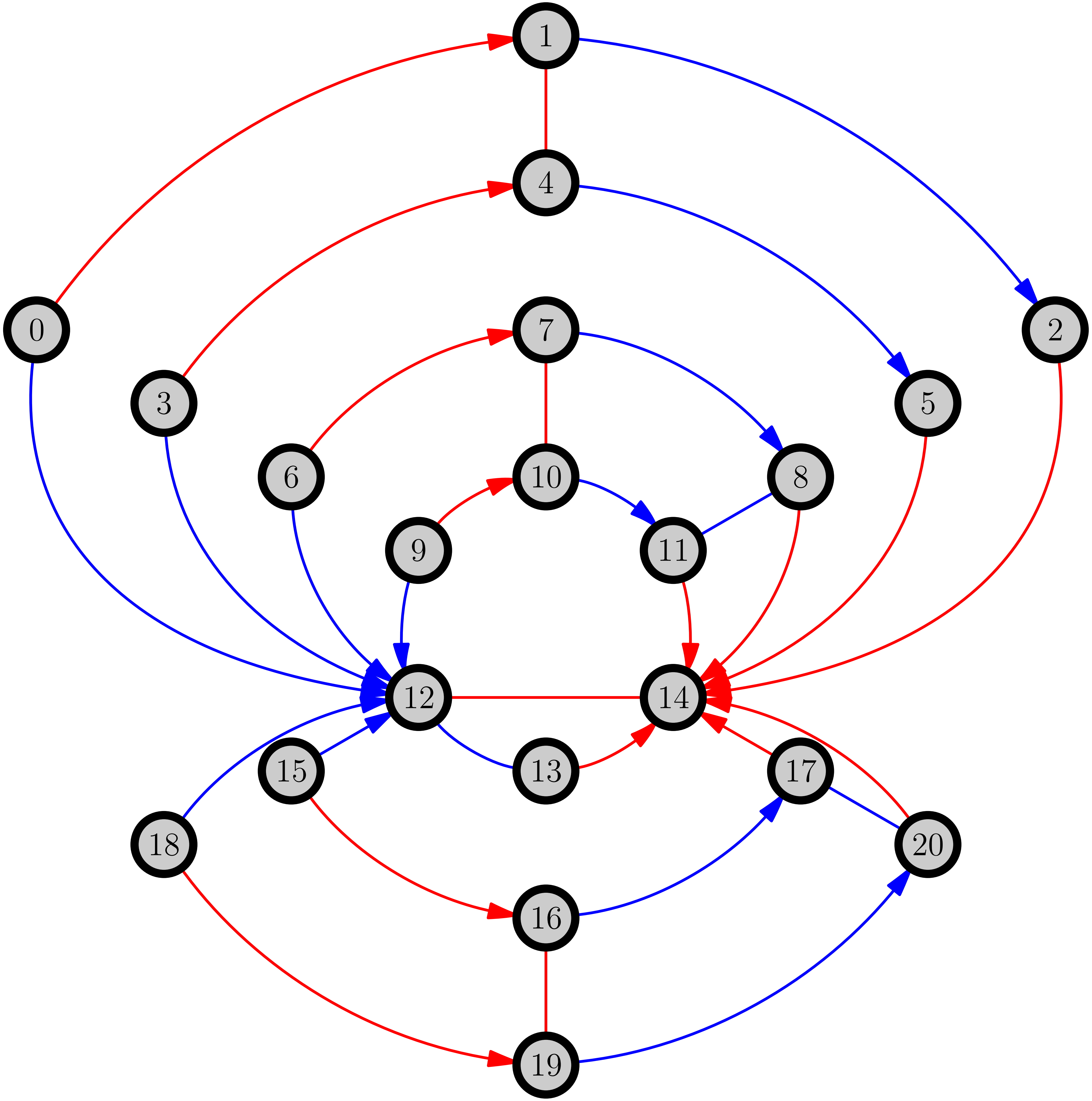

0
1
4
2
3
$0 = 1^3$
1
$2 = 1^4$
$3 = 1^5$
$4 = 1^2$

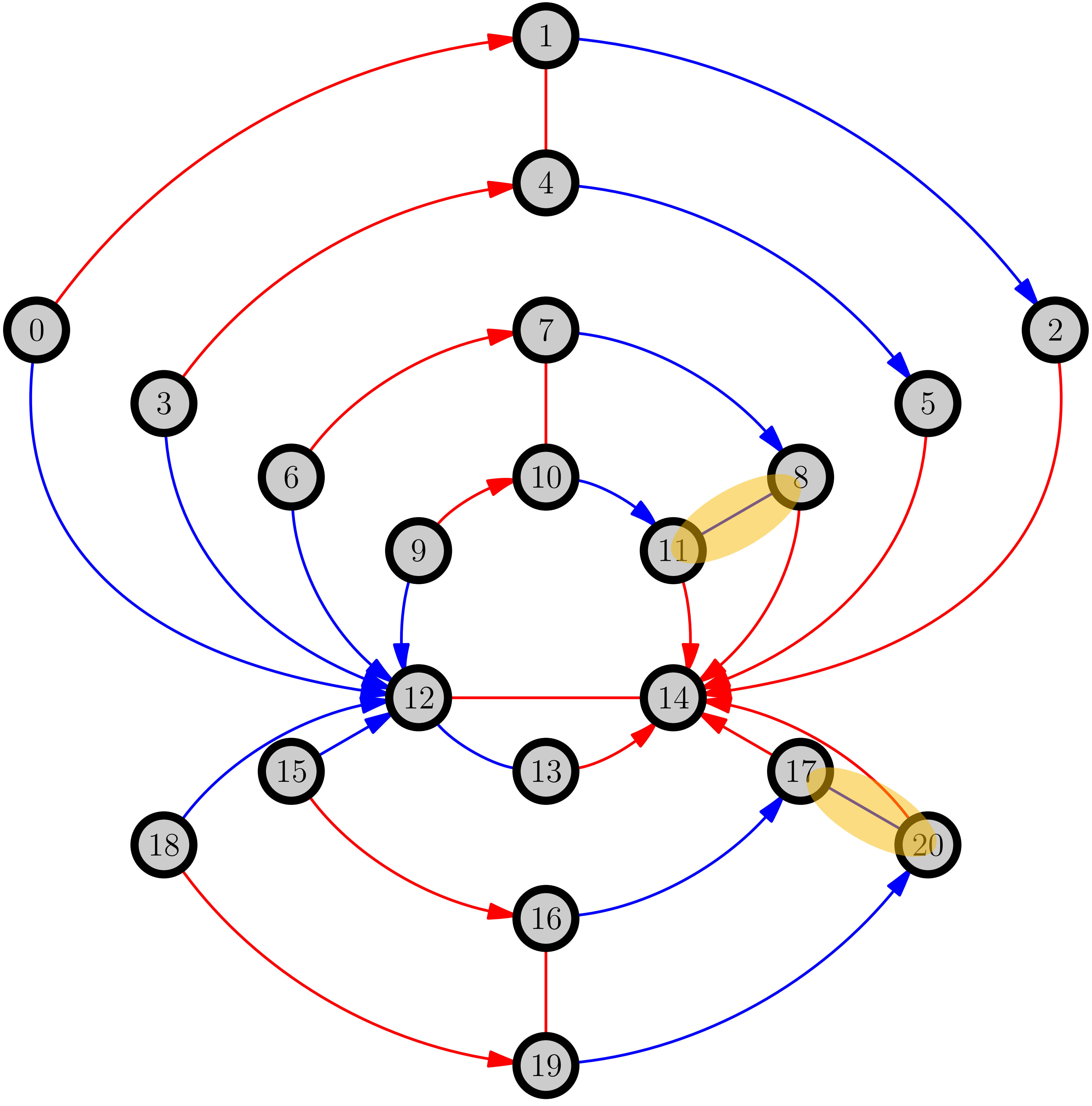


1
4
0
7
2
3
5
6
10
8
9
11
12
14
15
13
17
18
20
16
19

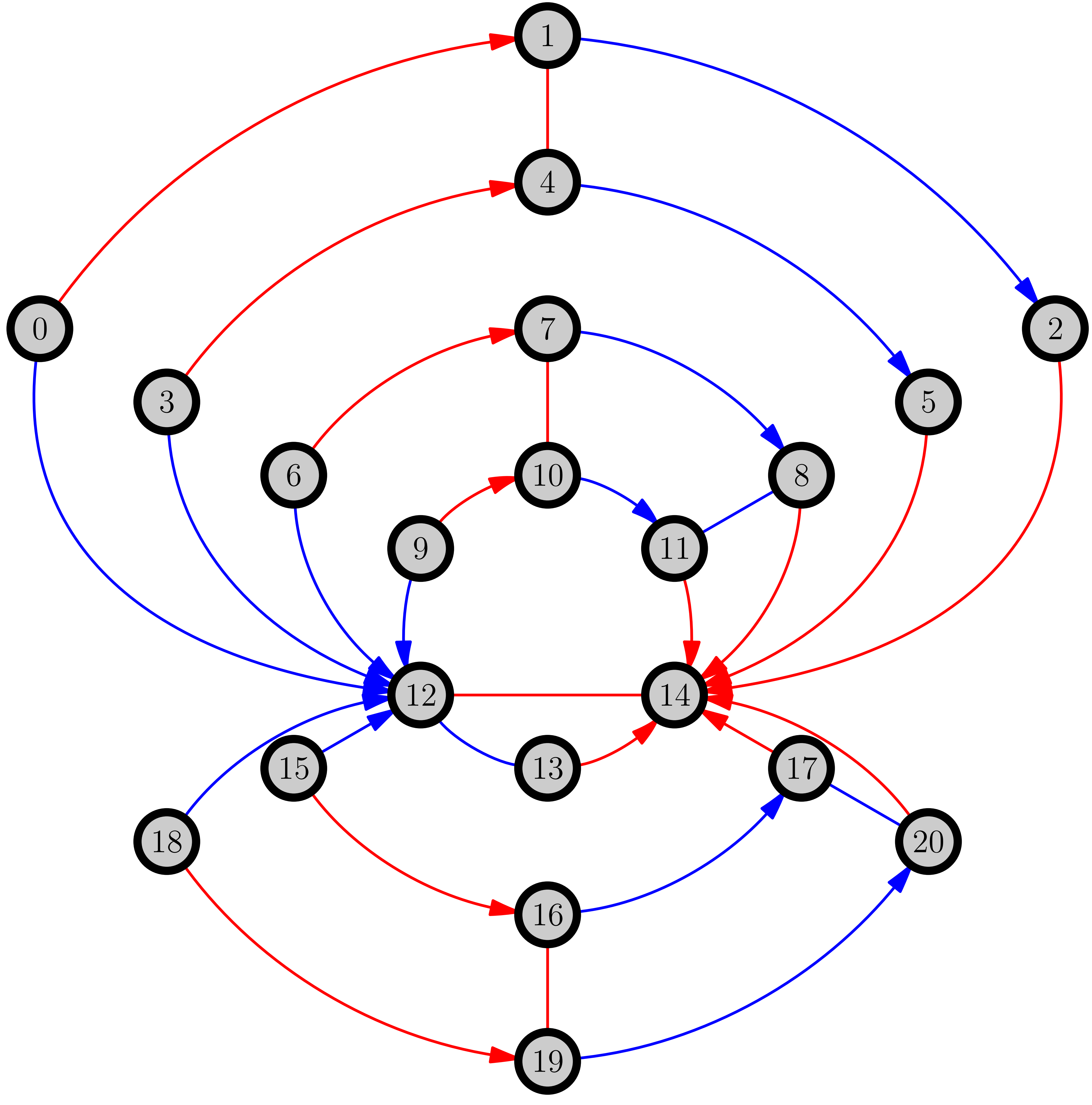

1
4
0
7
2
3
5
6
10
8
9
11
12
14
15
13
17
18
20
16
19


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

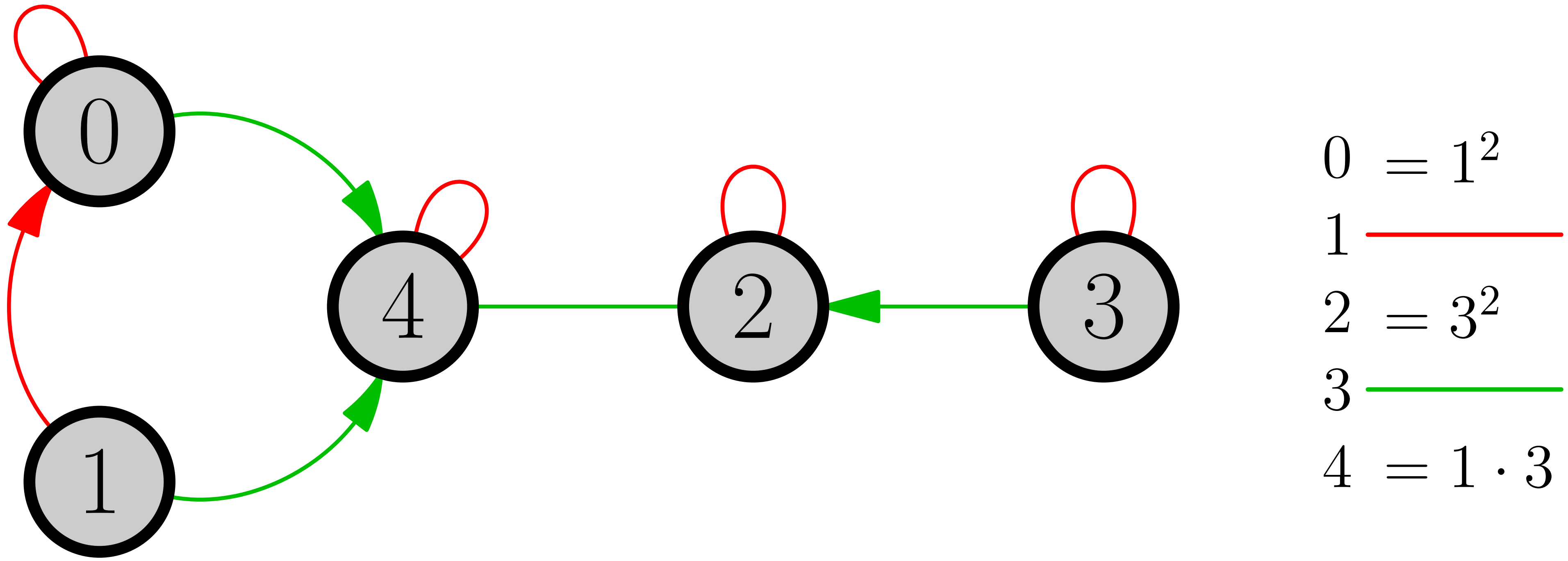

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



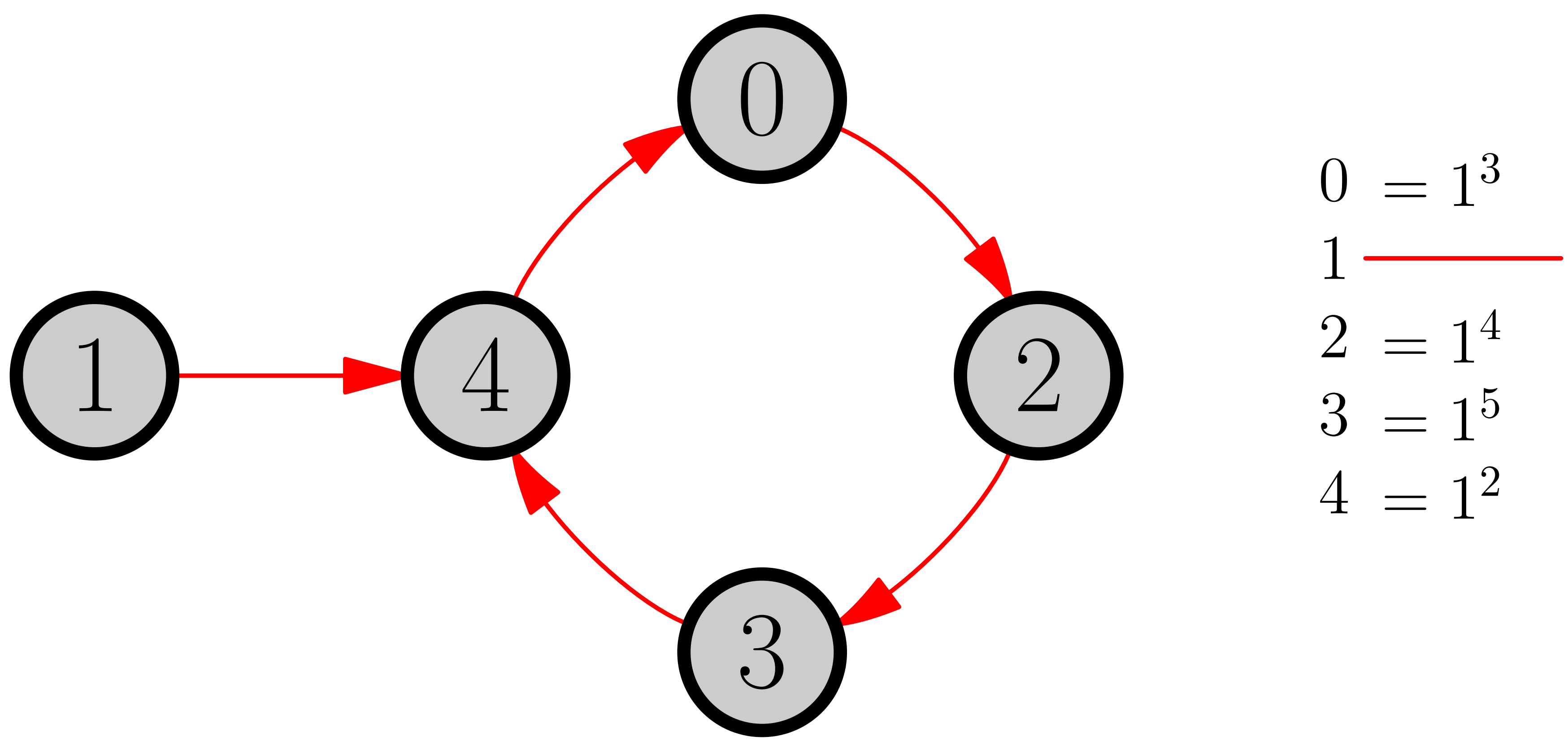
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20



0
1
2
3
4
$0 = 1^2$
1
$2 = 3^2$
3
$4 = 1 \cdot 3$



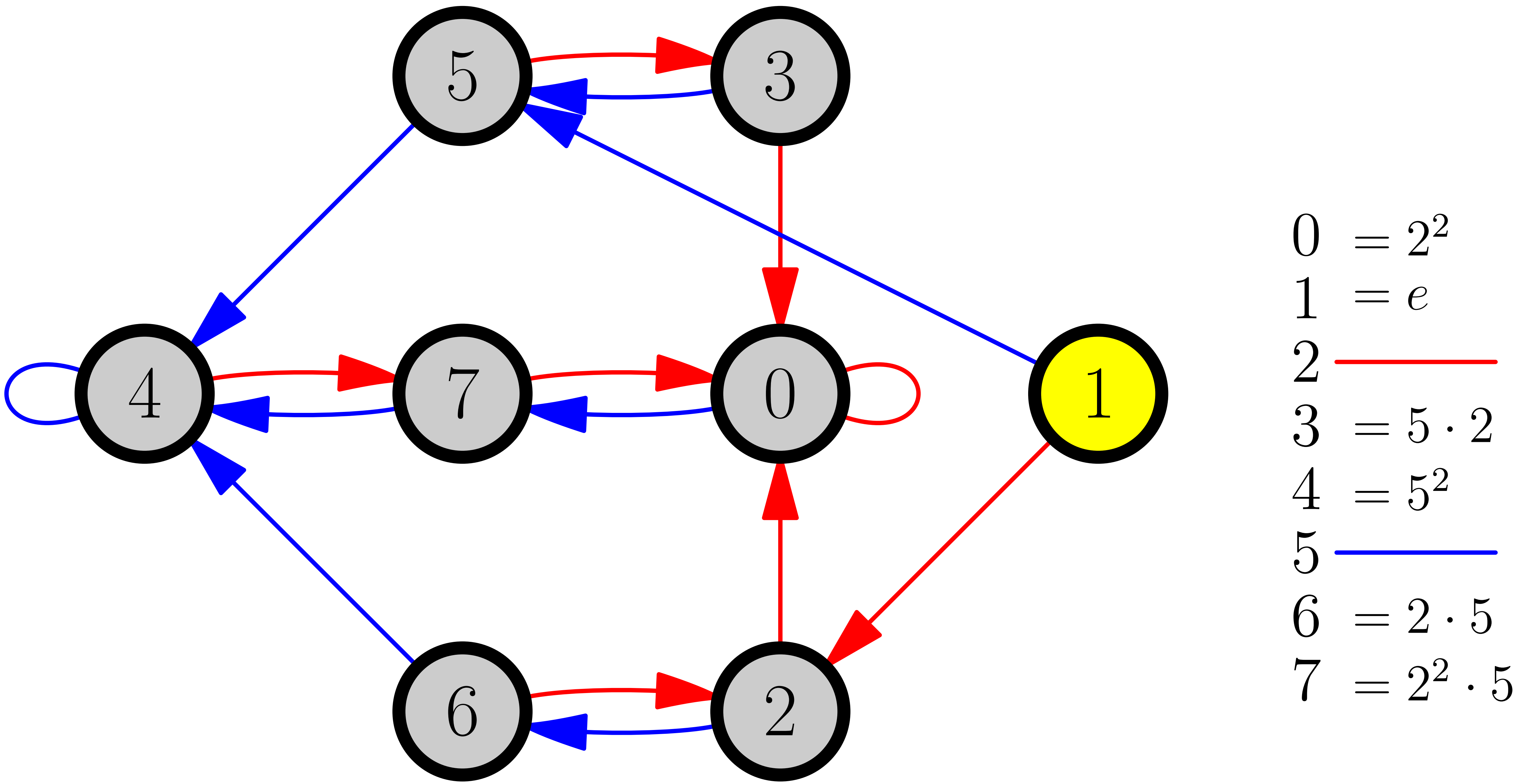
0
1
2
3
4
$0 = 1^3$
1
$2 = 1^4$
$3 = 1^5$
$4 = 1^2$

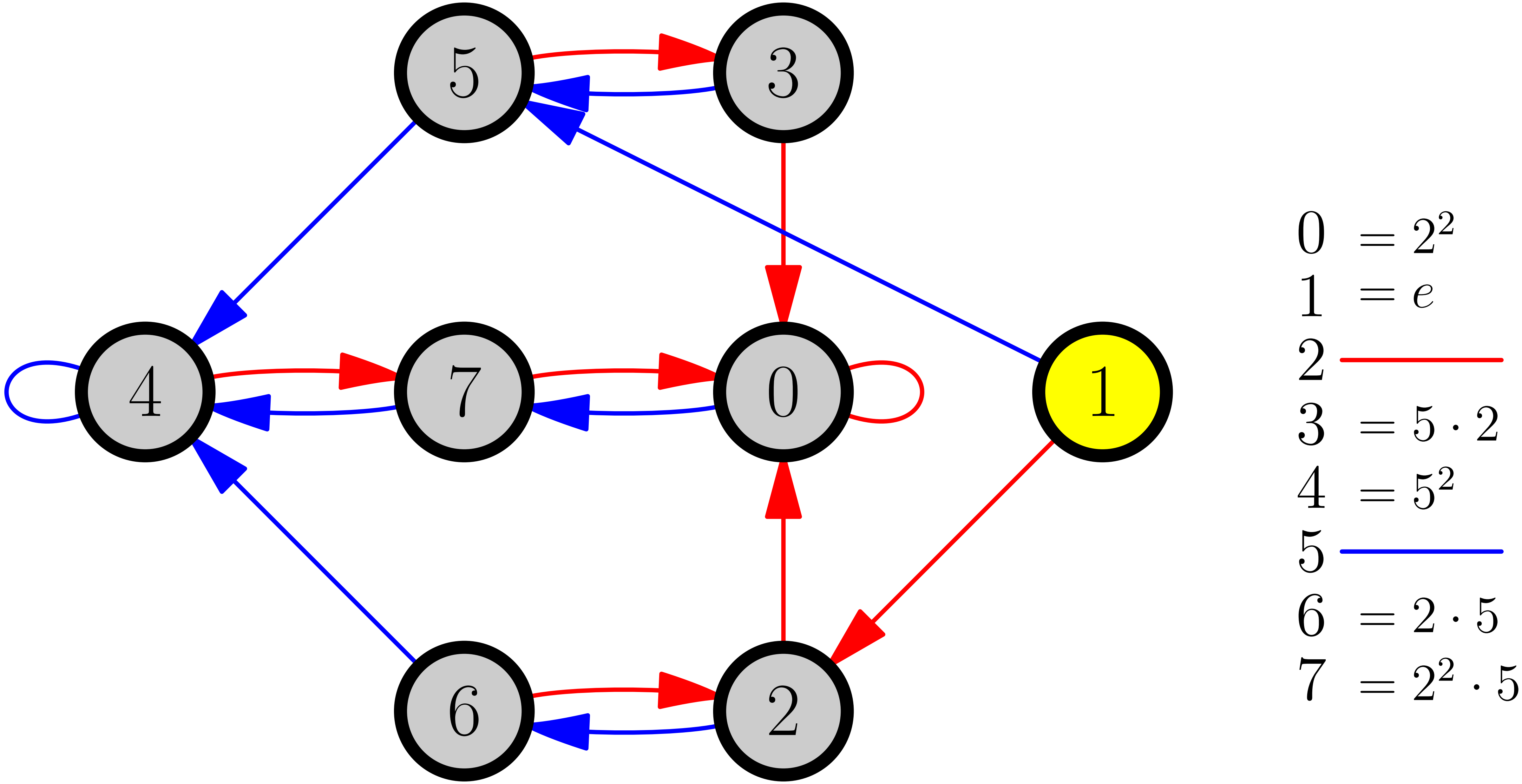
Five Definitions

1	A group is **a set S**	(set)
2	with **a binary operation * on S**	(magma)
3	that’s **associative,**	(semigroup)
4	has **an identity e,**	(monoid)
5	and has **inverses for every element.**	(group)

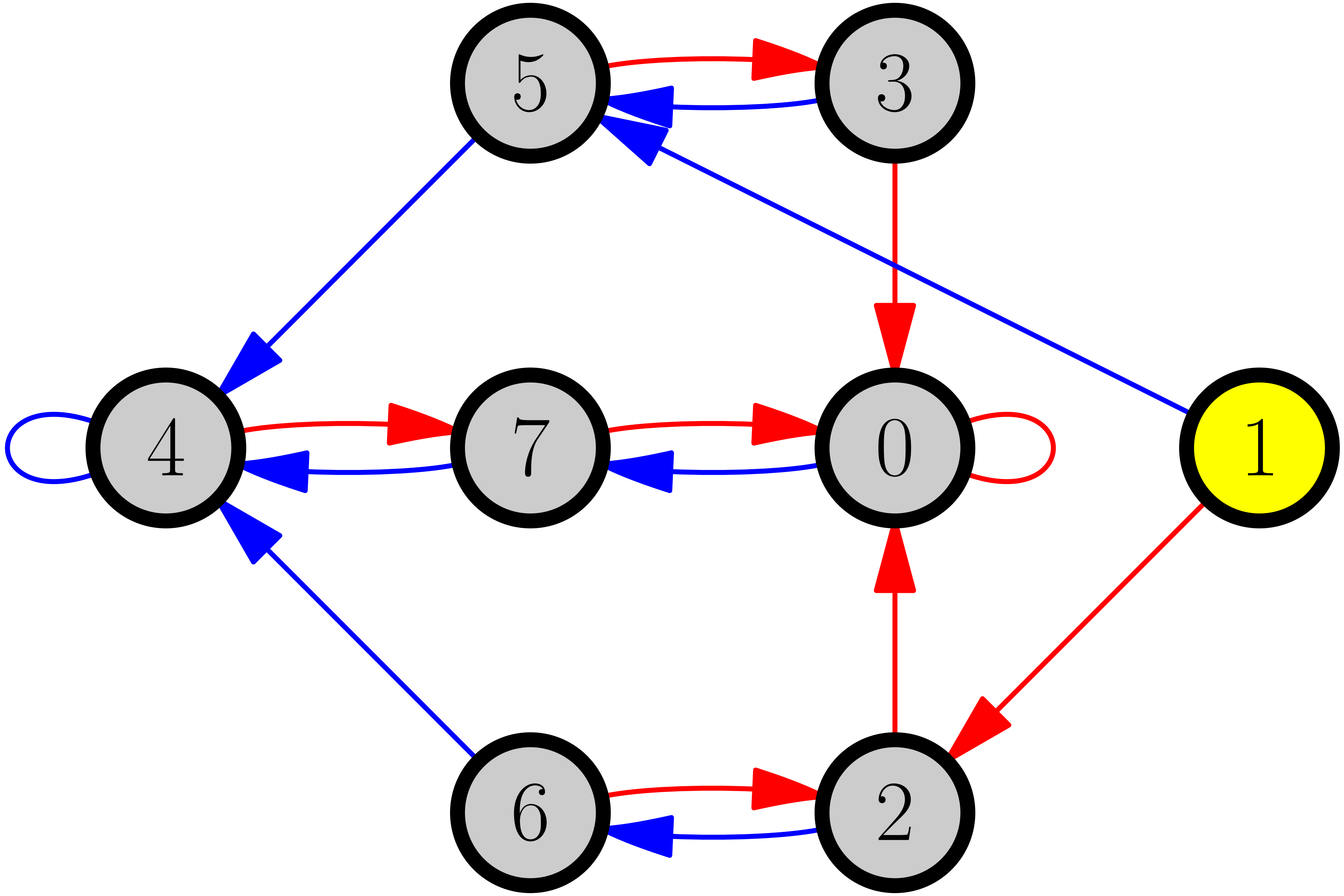
Five Definitions

1	A group is **a set S**	(set)
2	with **a binary operation * on S**	(magma)
3	that’s **associative,**	(semigroup)
4	has **an identity e,**	(monoid)
5	and has **inverses for every element.**	(group)


5
3
4
7
0
1
6
2
$0 = 2^2$
$1 = e$
2
$3 = 5 \cdot 2$
$4 = 5^2$
5
$6 = 2 \cdot 5$
$7 = 2^2 \cdot 5$

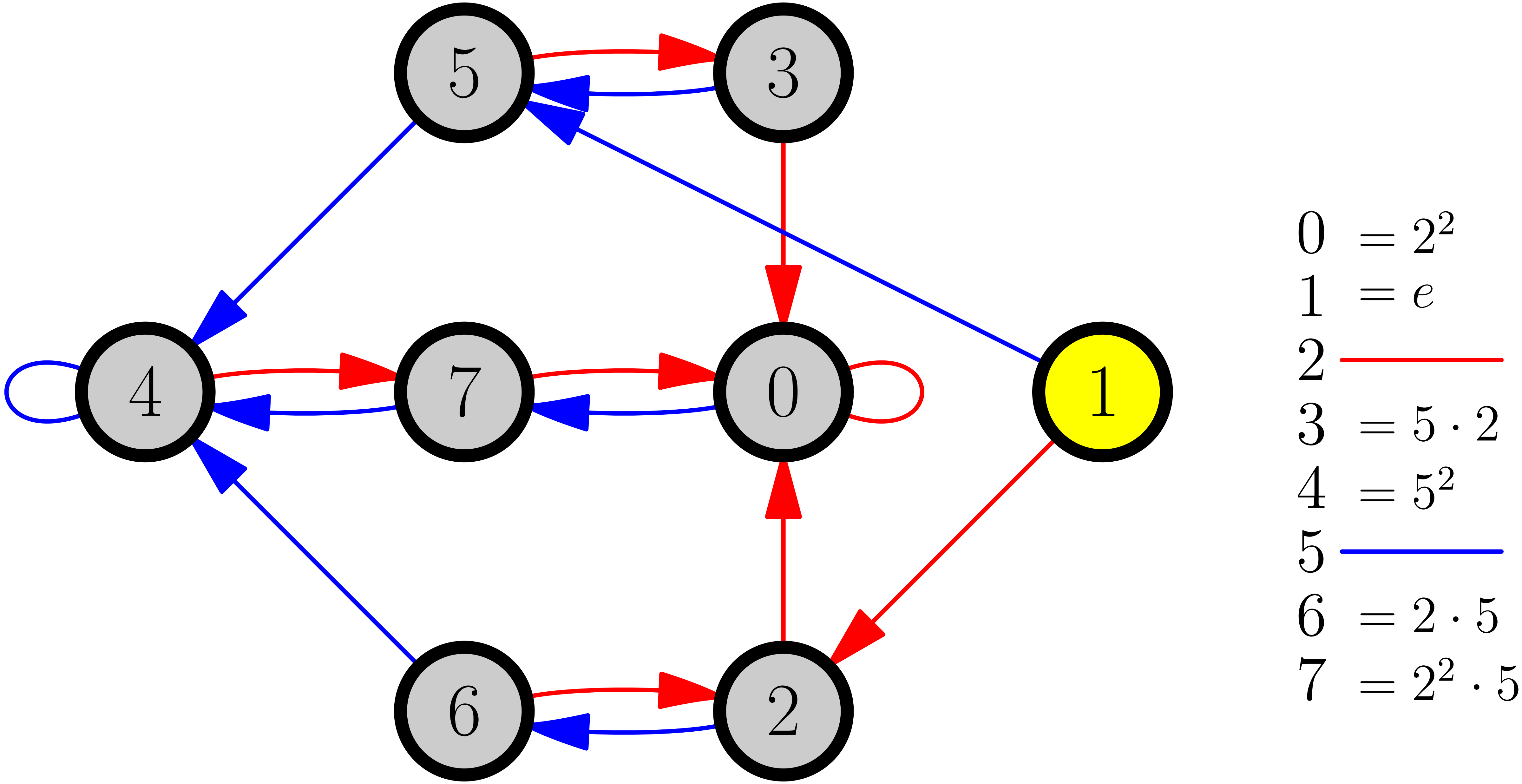


$$7 = 1 * 2 * 2 * 5 = 2 * 2 * 5$$



$0 \; = 2^2$
$1 \; = e$
2
$3 \; = 5 \cdot 2$
$4 \; = 5^2$
5
$6 \; = 2 \cdot 5$
$7 \; = 2^2 \cdot 5$

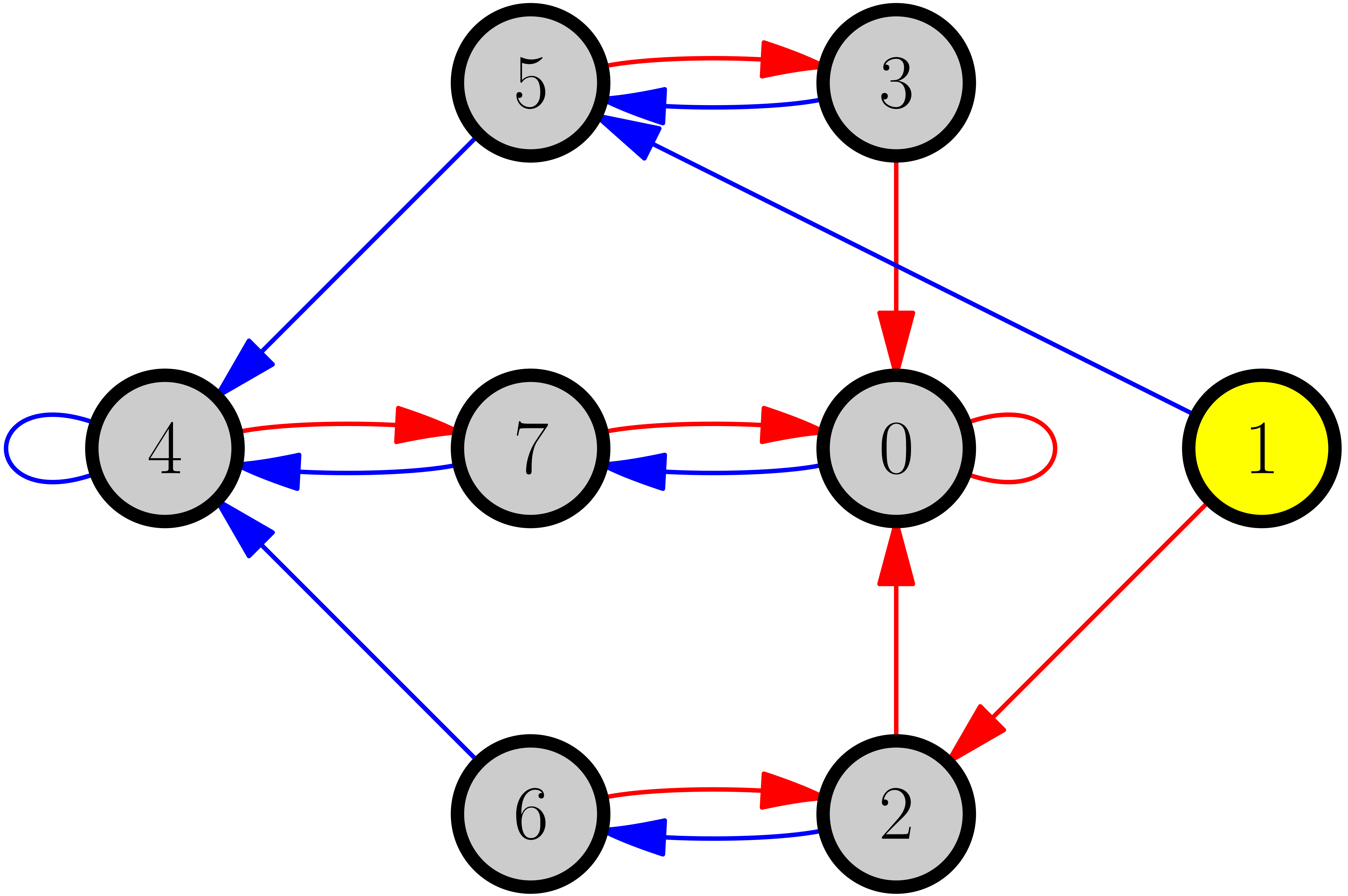
$$7 = 1 * 2 * 2 * 5 = 2 * 2 * 5$$
$$7 = 1 * 5 * 5 * 2 = 5 * 5 * 2$$

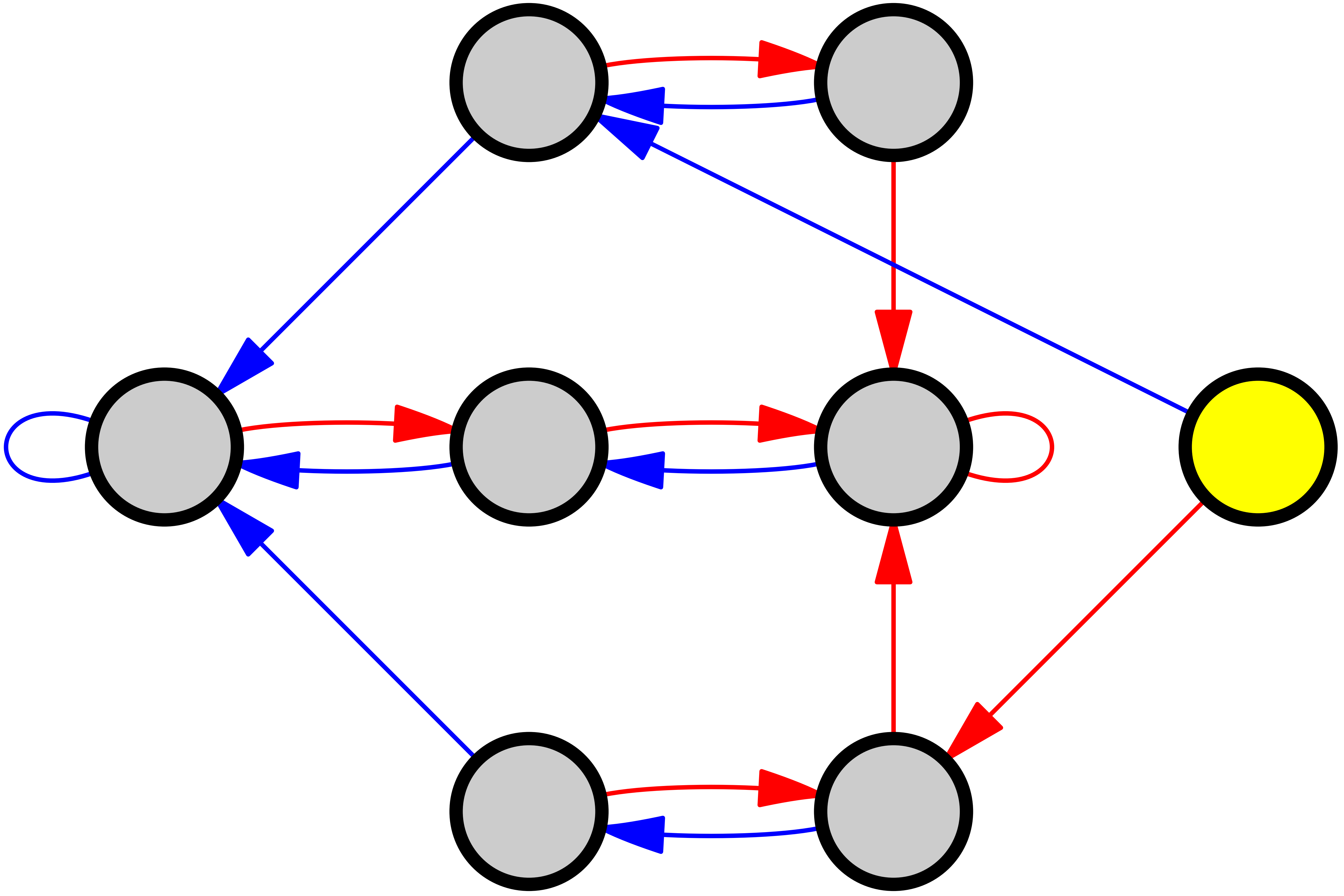


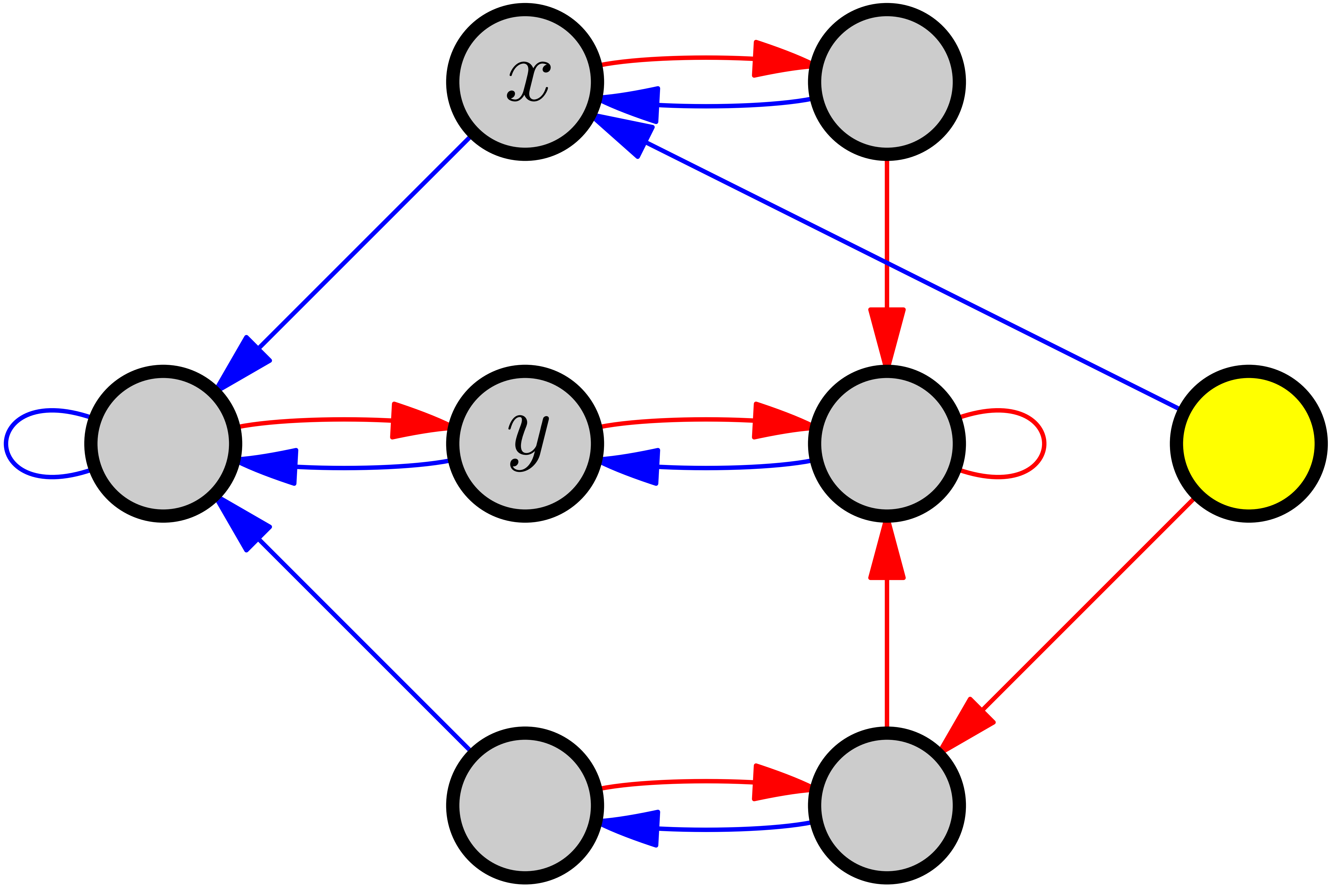
$$7 = 1 * 2 * 2 * 5 = 2 * 2 * 5$$

$$7 = 1 * 5 * 5 * 2 = 5 * 5 * 2$$

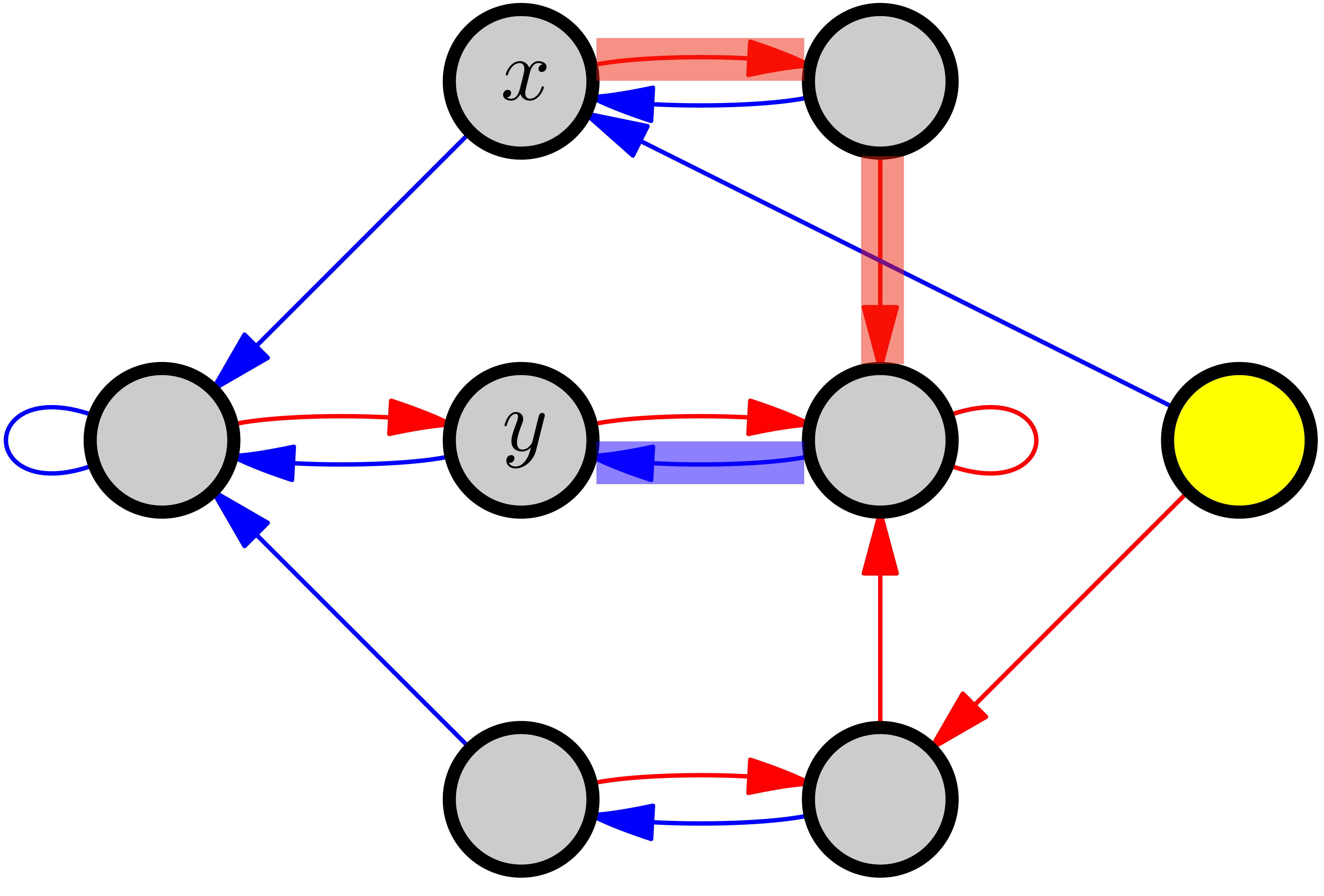
$$\therefore 2 * 2 * 5 = 5 * 5 * 2$$

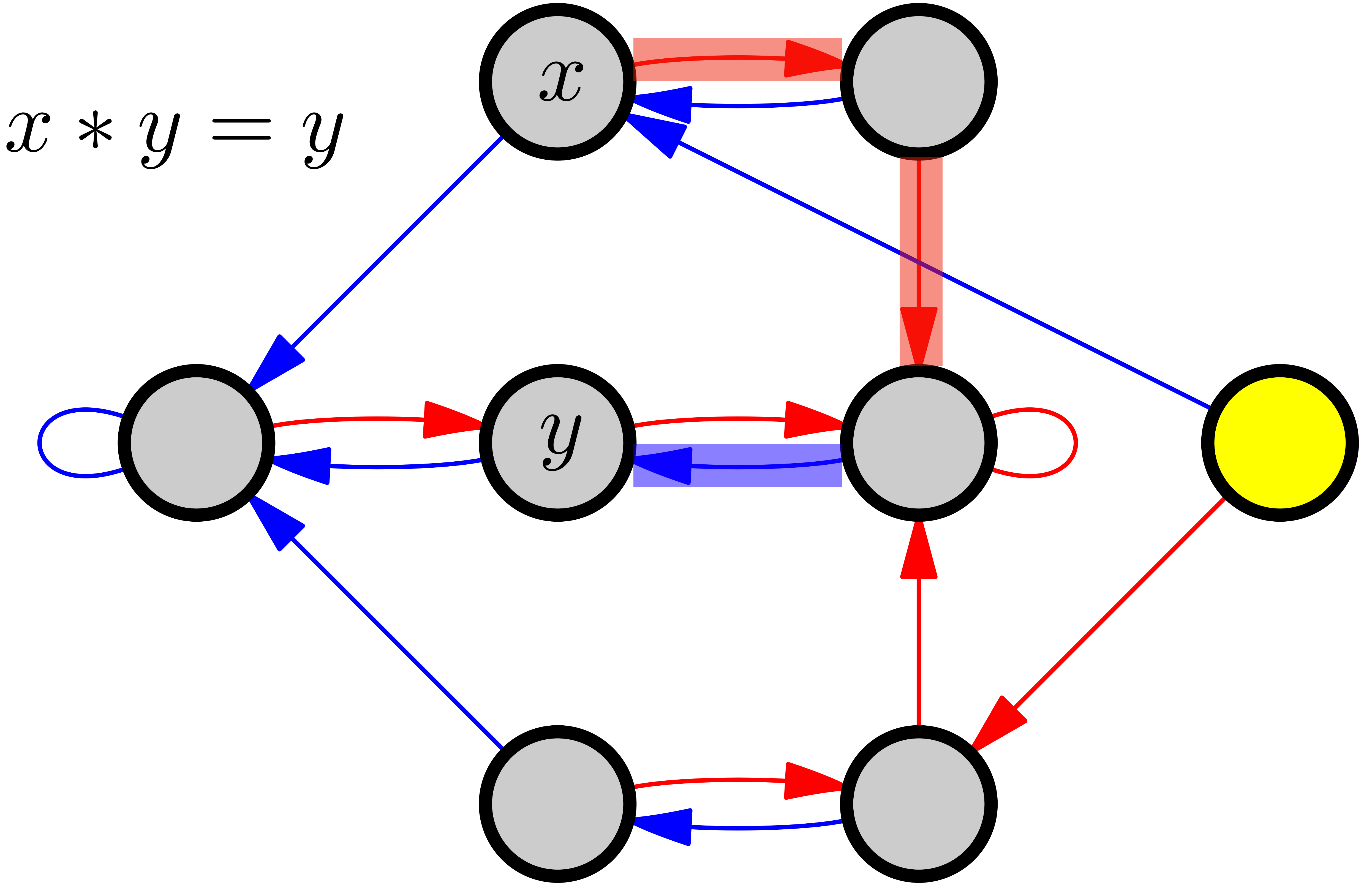

5
3
4
7
0
1
6
2



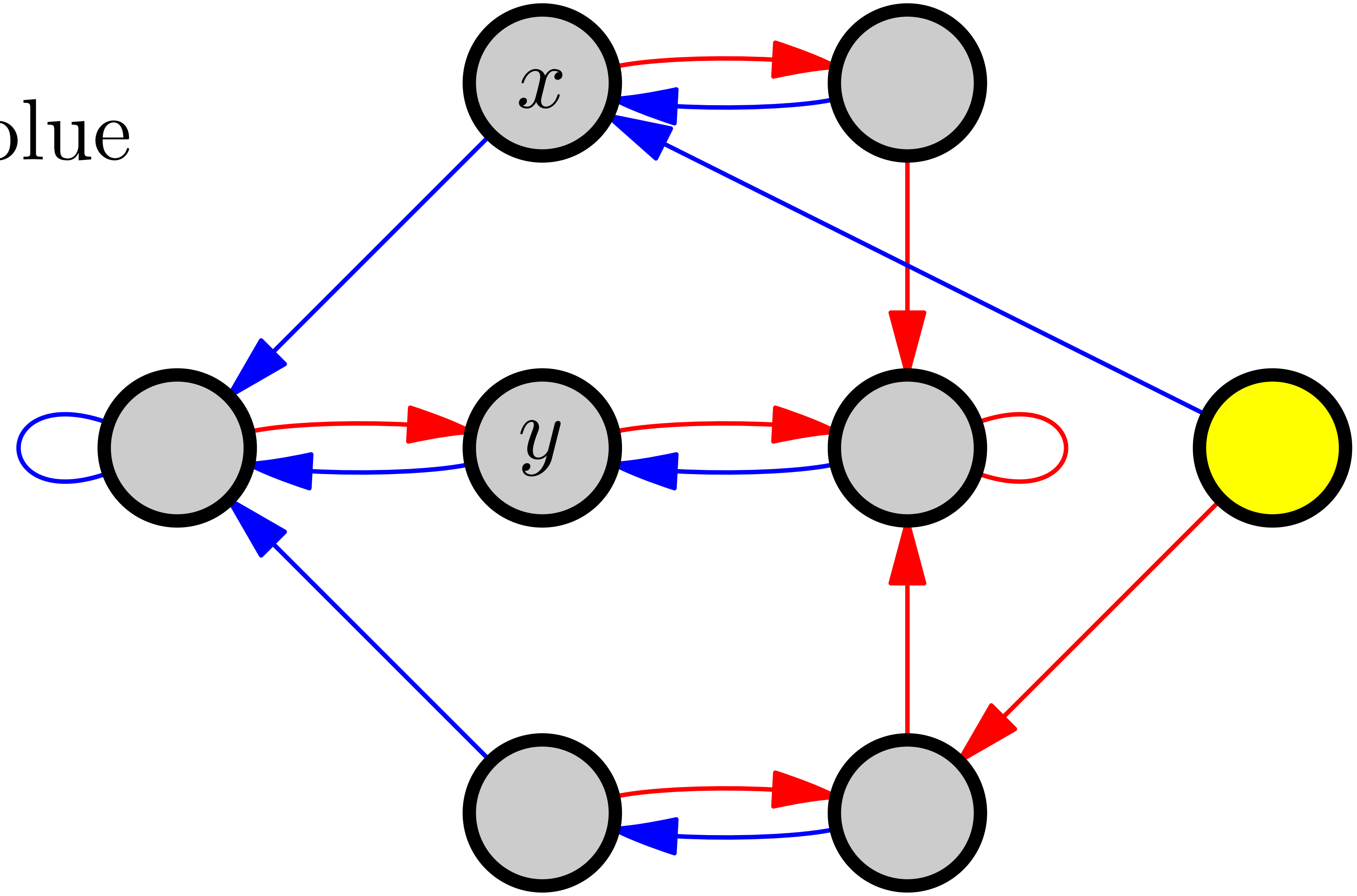


x
y


x
y

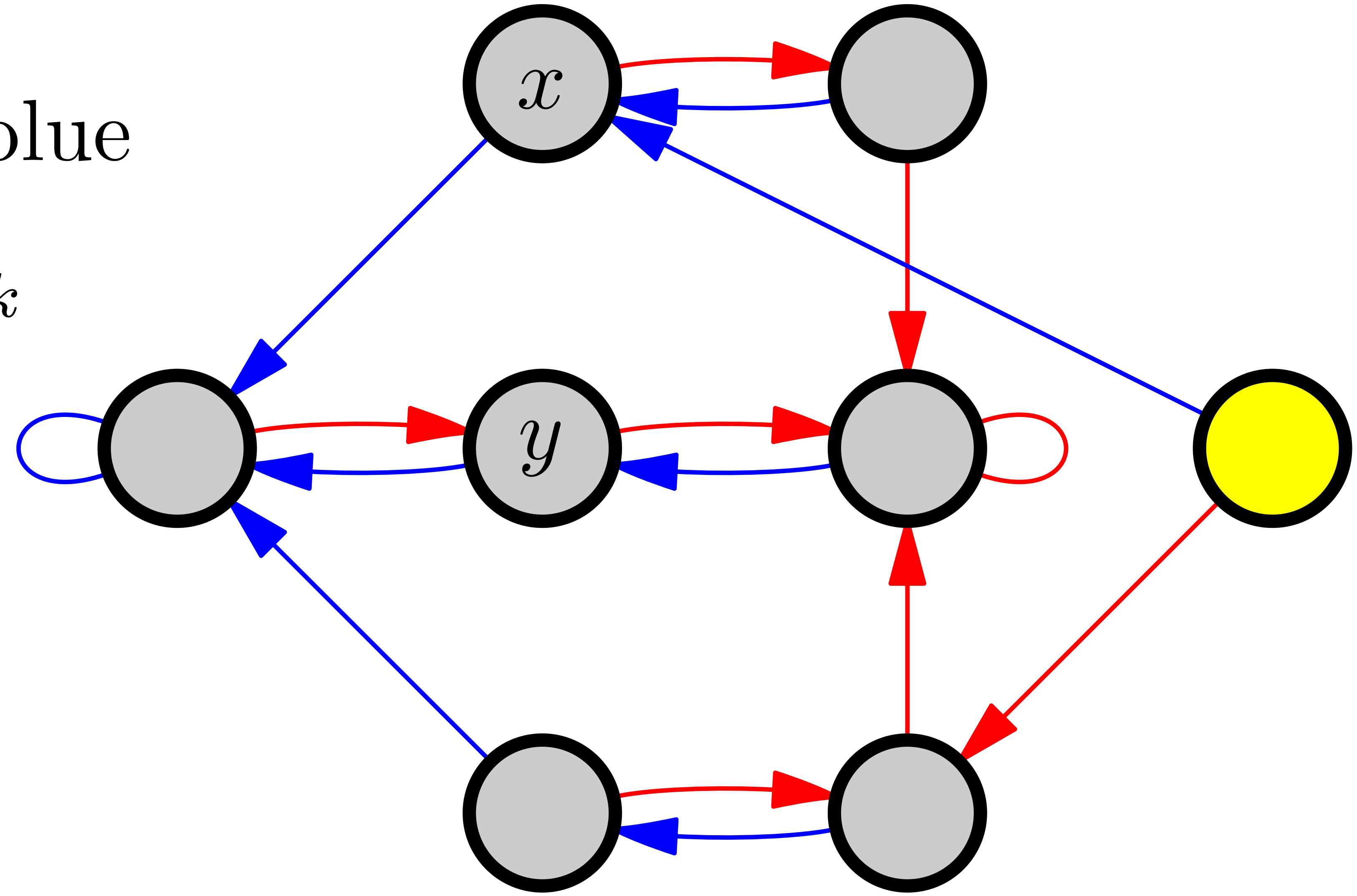

$x * y = y$
x
y

$$y = 1 * \mathrm{red} * \mathrm{red} * \mathrm{blue}$$



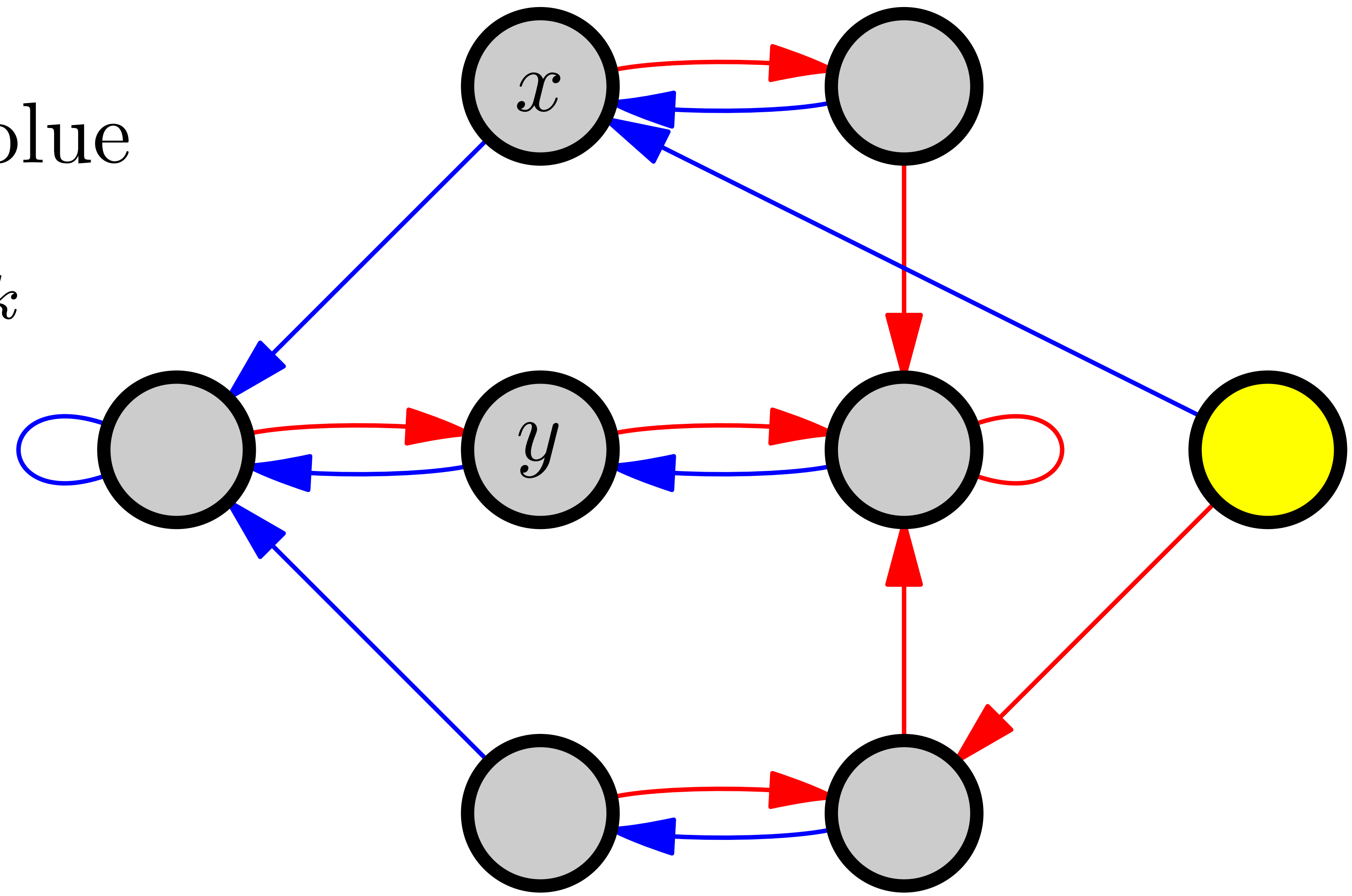
$$y = 1 * \mathrm{red} * \mathrm{red} * \mathrm{blue}$$

$$y = 1 * g_1 * \cdots * g_k$$



$$y = 1 * \mathrm{red} * \mathrm{red} * \mathrm{blue}$$

$$y = 1 * g_1 * \cdots * g_k$$

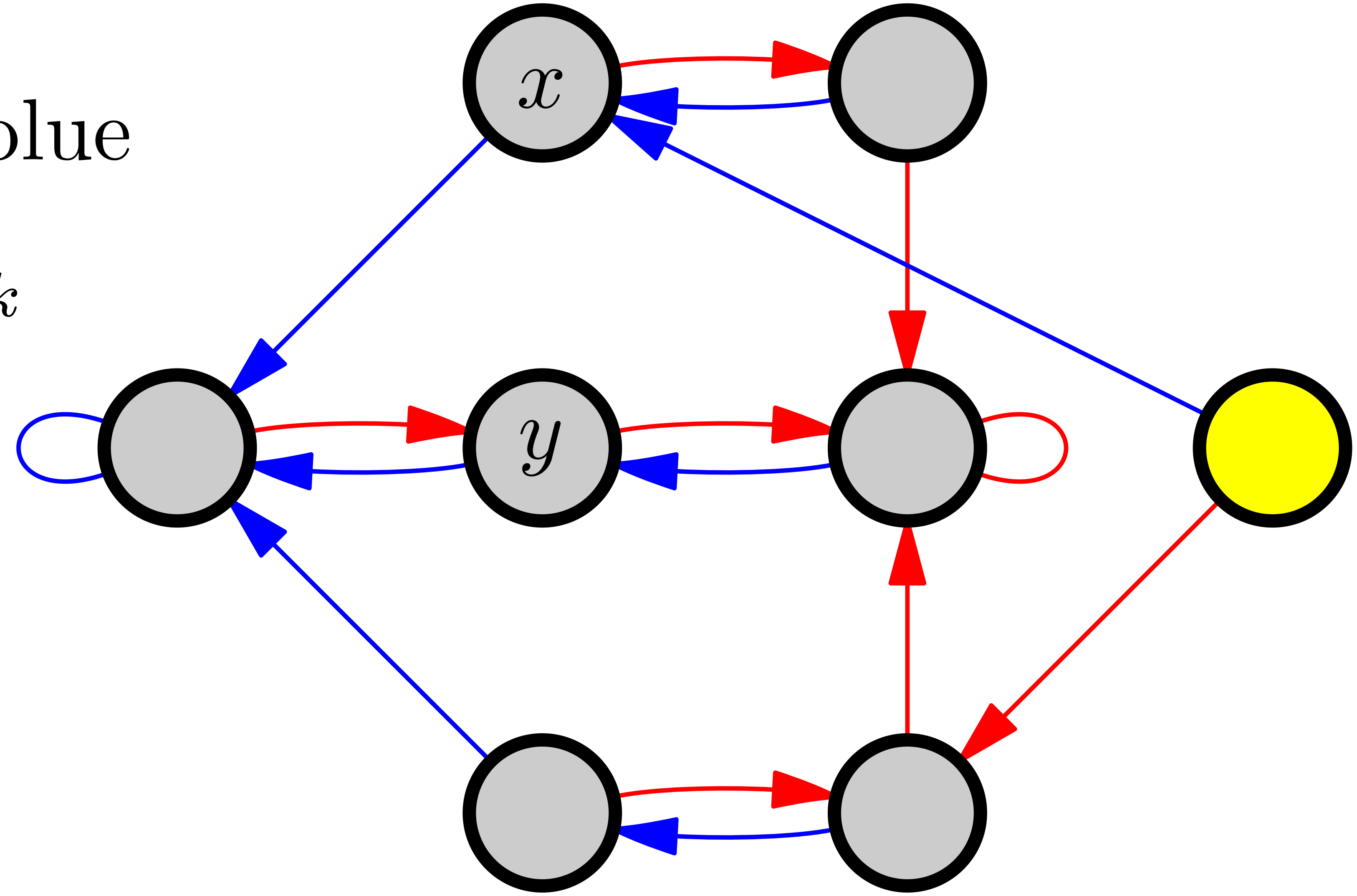


$$x * y = x * (1 * g_1 * \cdots * g_k)$$

substitution

$$y = 1 * \mathrm{red} * \mathrm{red} * \mathrm{blue}$$

$$y = 1 * g_1 * \cdots * g_k$$

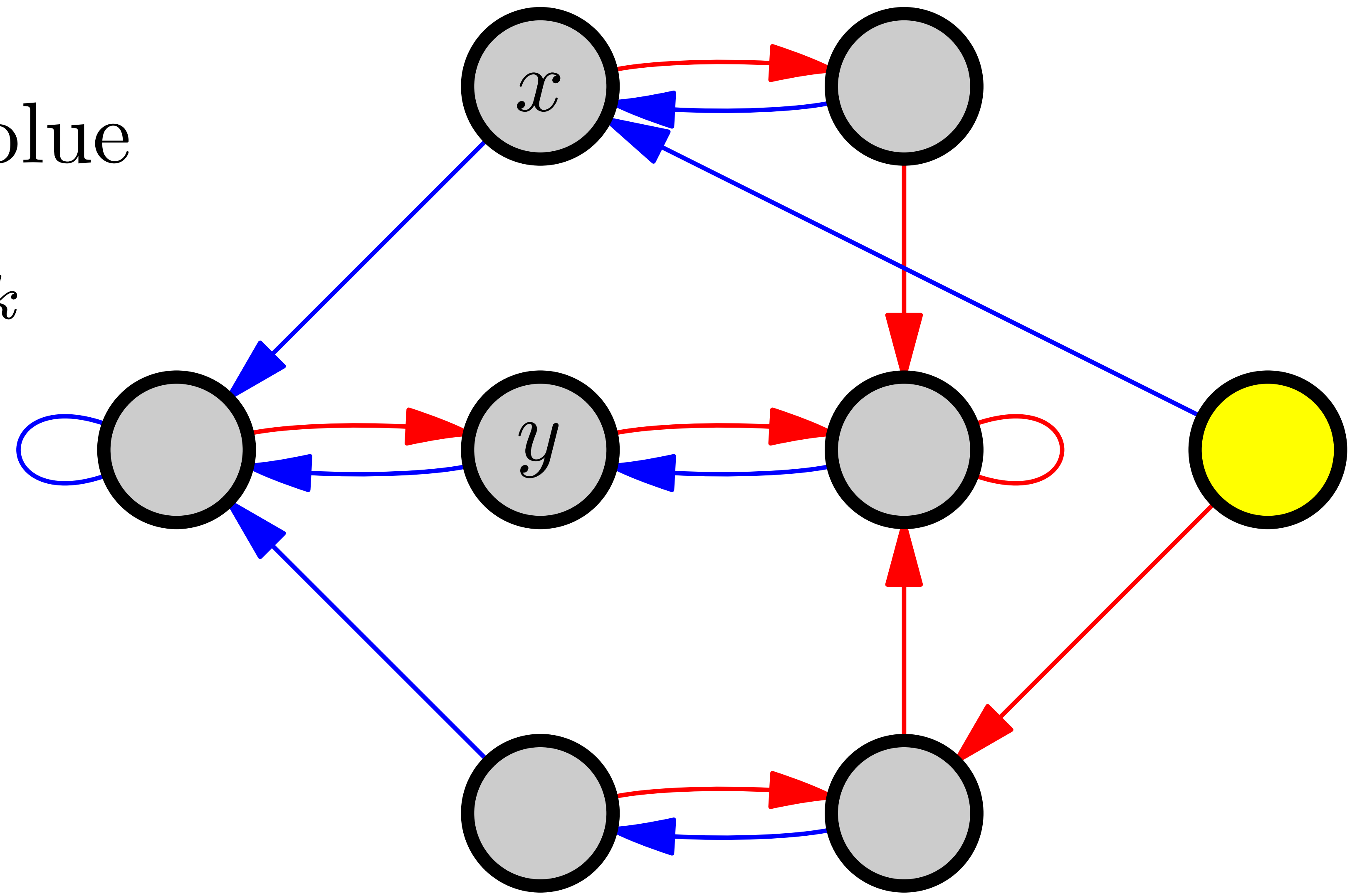


$$x * y = x * (1 * g_1 * \cdots * g_k) \qquad \text{substitution}$$

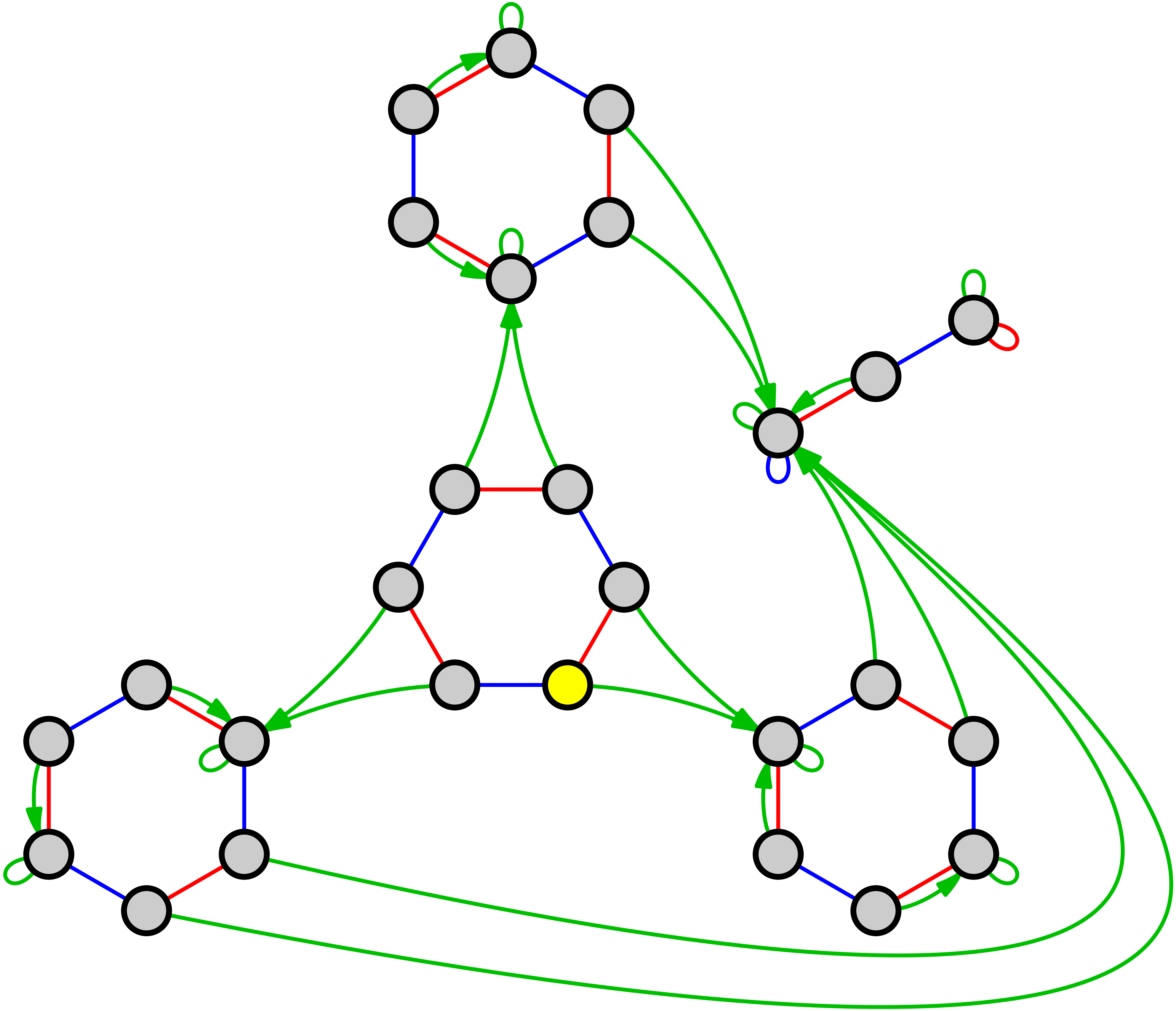
$$= x * (g_1 * \cdots * g_k) \qquad \text{identity}$$

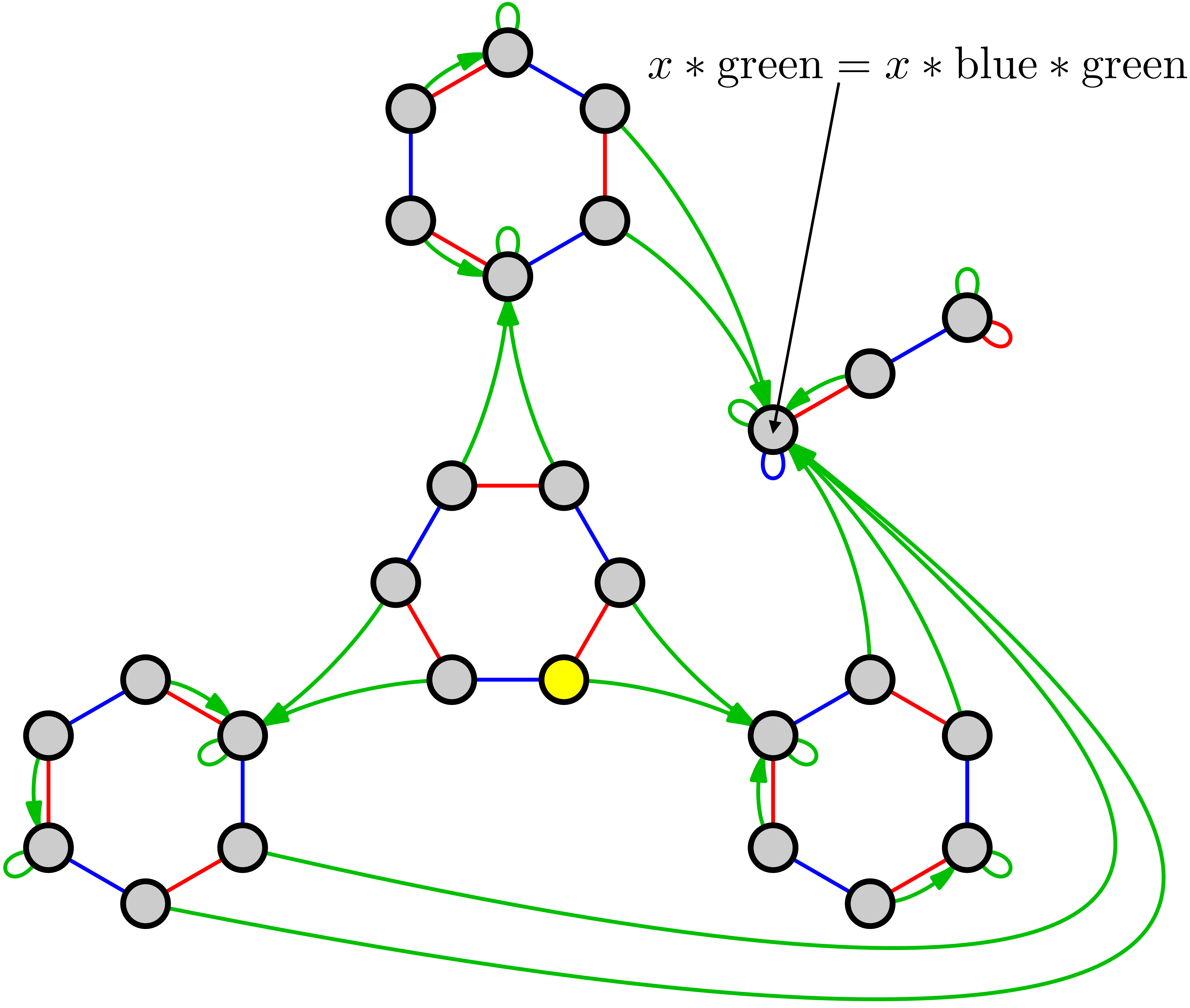
$$y = 1 * \mathrm{red} * \mathrm{red} * \mathrm{blue}$$

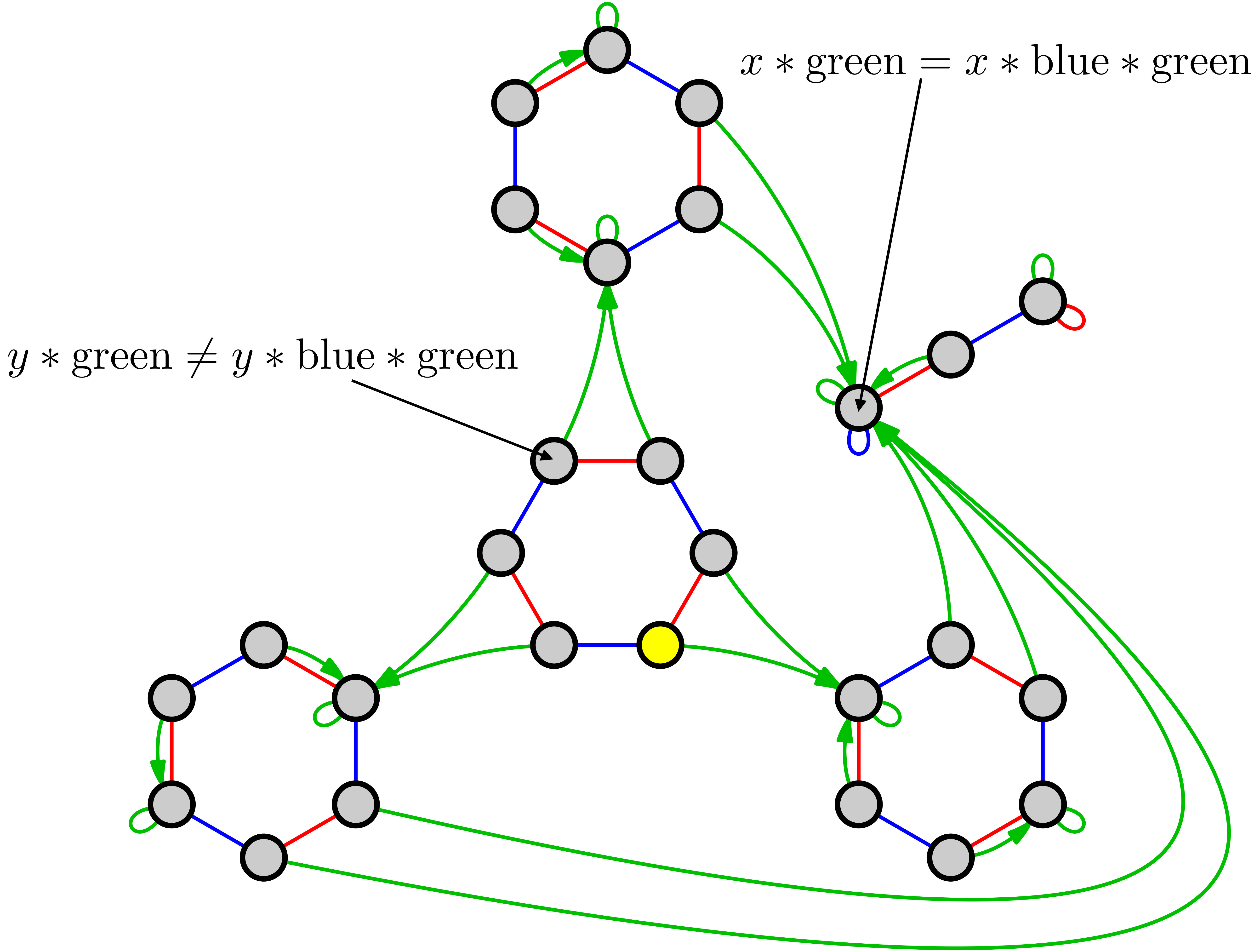
$$y = 1 * g_1 * \cdots * g_k$$



$$\begin{aligned} x * y &= x * (1 * g_1 * \cdots * g_k) && \text{substitution} \\ &= x * (g_1 * \cdots * g_k) && \text{identity} \\ &= (\cdots(x * g_1) * \cdots) * g_k) && \text{associativity} \end{aligned}$$




$x * \mathrm{green} = x * \mathrm{blue} * \mathrm{green}$


$x * \text{green} = x * \text{blue} * \text{green}$
$y * \text{green} \neq y * \text{blue} * \text{green}$

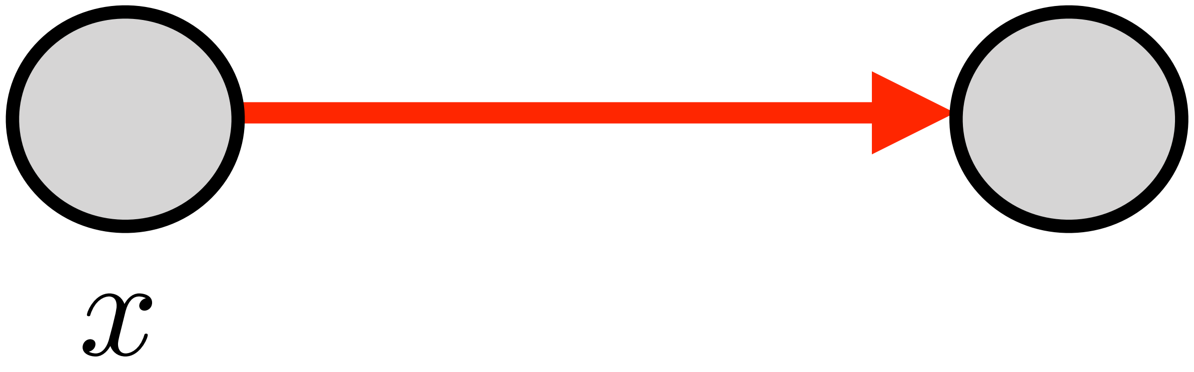
Five Definitions

1	A group is **a set S**	(set)
2	with **a binary operation * on S**	(magma)
3	that's **associative,**	(semigroup)
4	has **an identity e,**	(monoid)
5	and has **inverses for every element.**	(group)

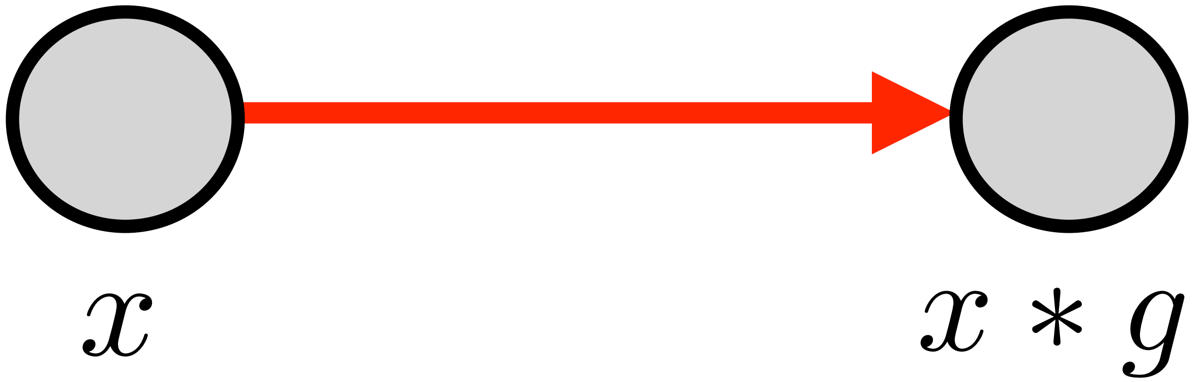
Five Definitions

1	A group is **a set S**	(set)
2	with **a binary operation * on S**	(magma)
3	that’s **associative,**	(semigroup)
4	has **an identity e,**	(monoid)
5	and has **inverses for every element.**	(group)

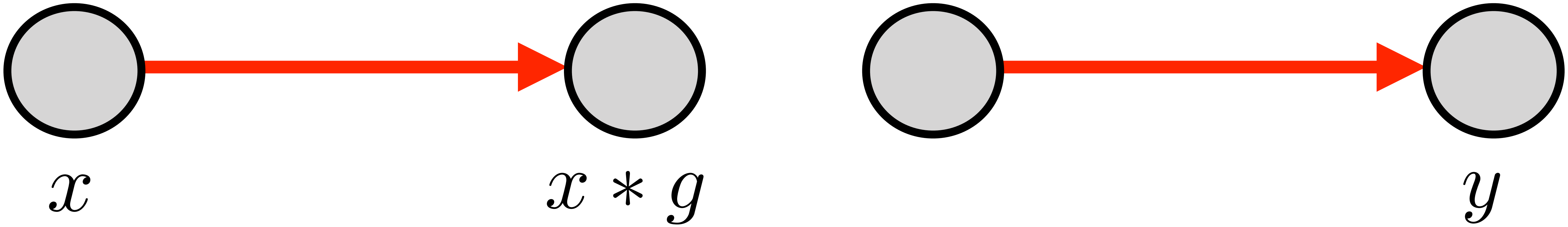
Invertibility



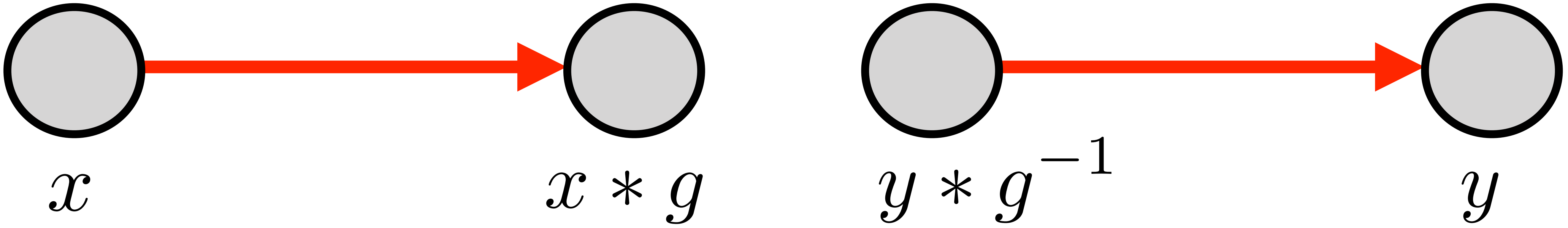
Invertibility



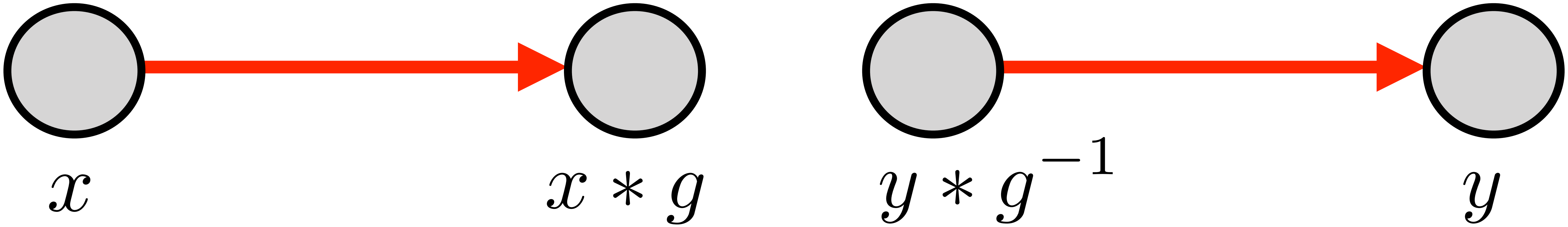
Invertibility



Invertibility

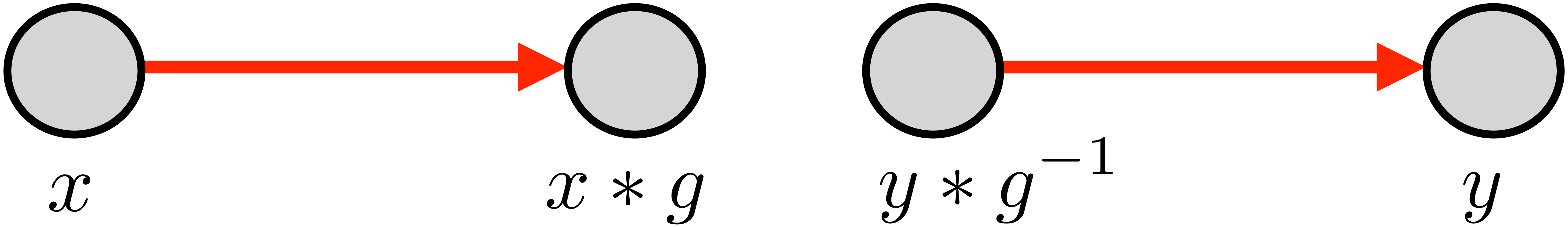


Invertibility



Location Invariance

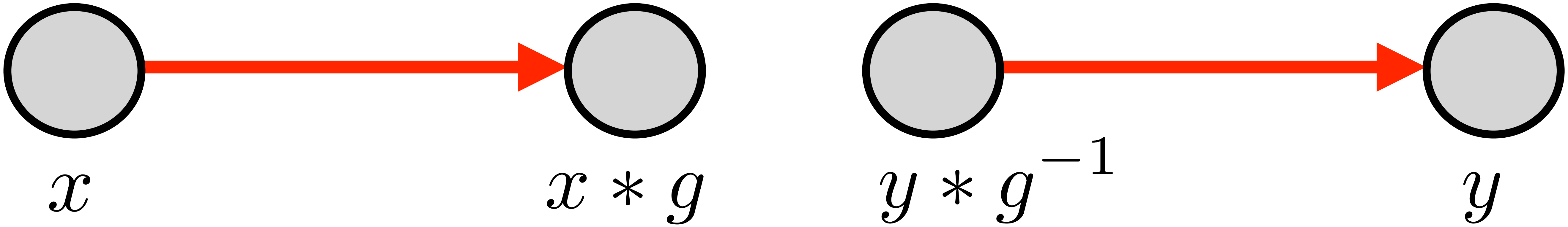
Invertibility



Location Invariance

$$x * (g_1 * \cdots * g_k) = x * (g'_1 * \cdots * g'_{k'})$$

Invertibility

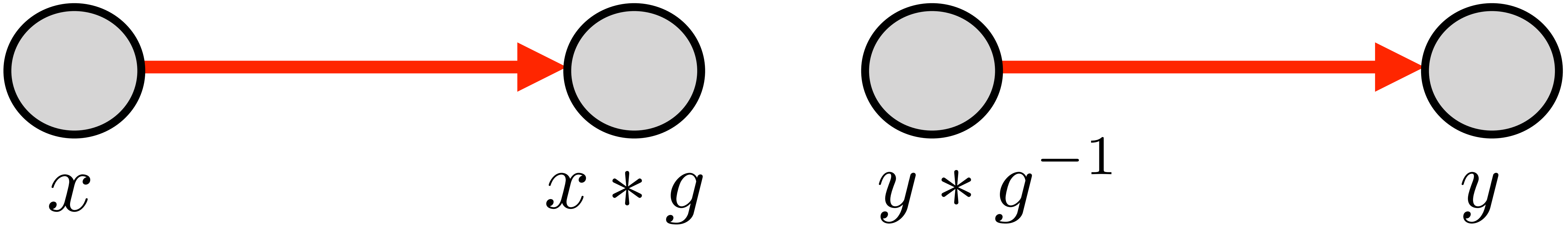


Location Invariance

$$x * (g_1 * \cdots * g_k) = x * (g'_1 * \cdots * g'_{k'})$$

$$(y * x^{-1}) * x * g_1 * \cdots * g_k = (y * x^{-1}) * x * (g'_1 * \cdots * g'_{k'})$$

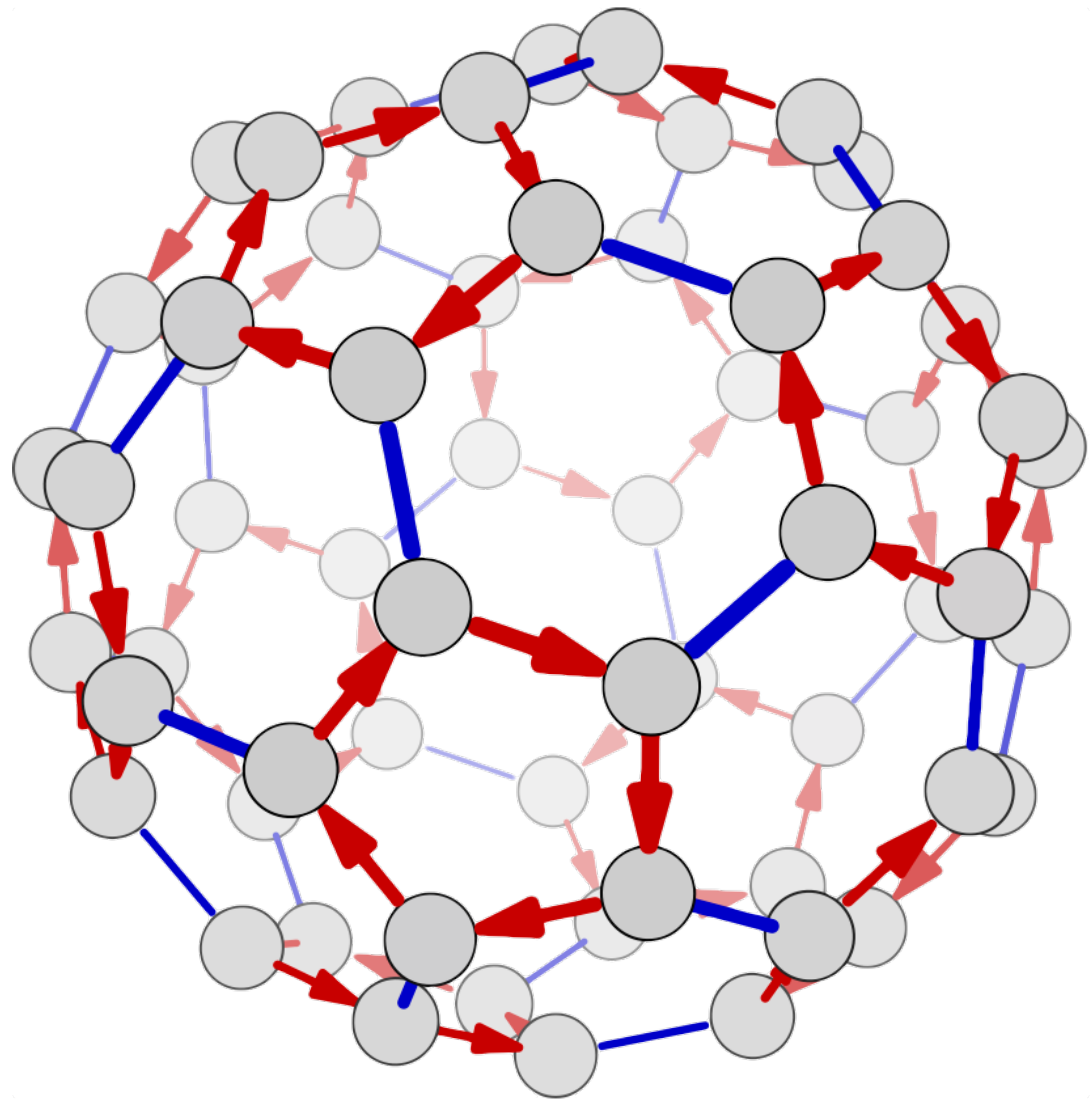
Invertibility



Location Invariance

$$x * (g_1 * \cdots * g_k) = x * (g'_1 * \cdots * g'_{k'})$$
$$(y * x^{-1}) * x * g_1 * \cdots * g_k = (y * x^{-1}) * x * (g'_1 * \cdots * g'_{k'})$$
$$y * (g_1 * \cdots * g_k) = y * (g'_1 * \cdots * g'_{k'})$$

The Surprising Pedagogical Value and Versatility of Cayley Graphs

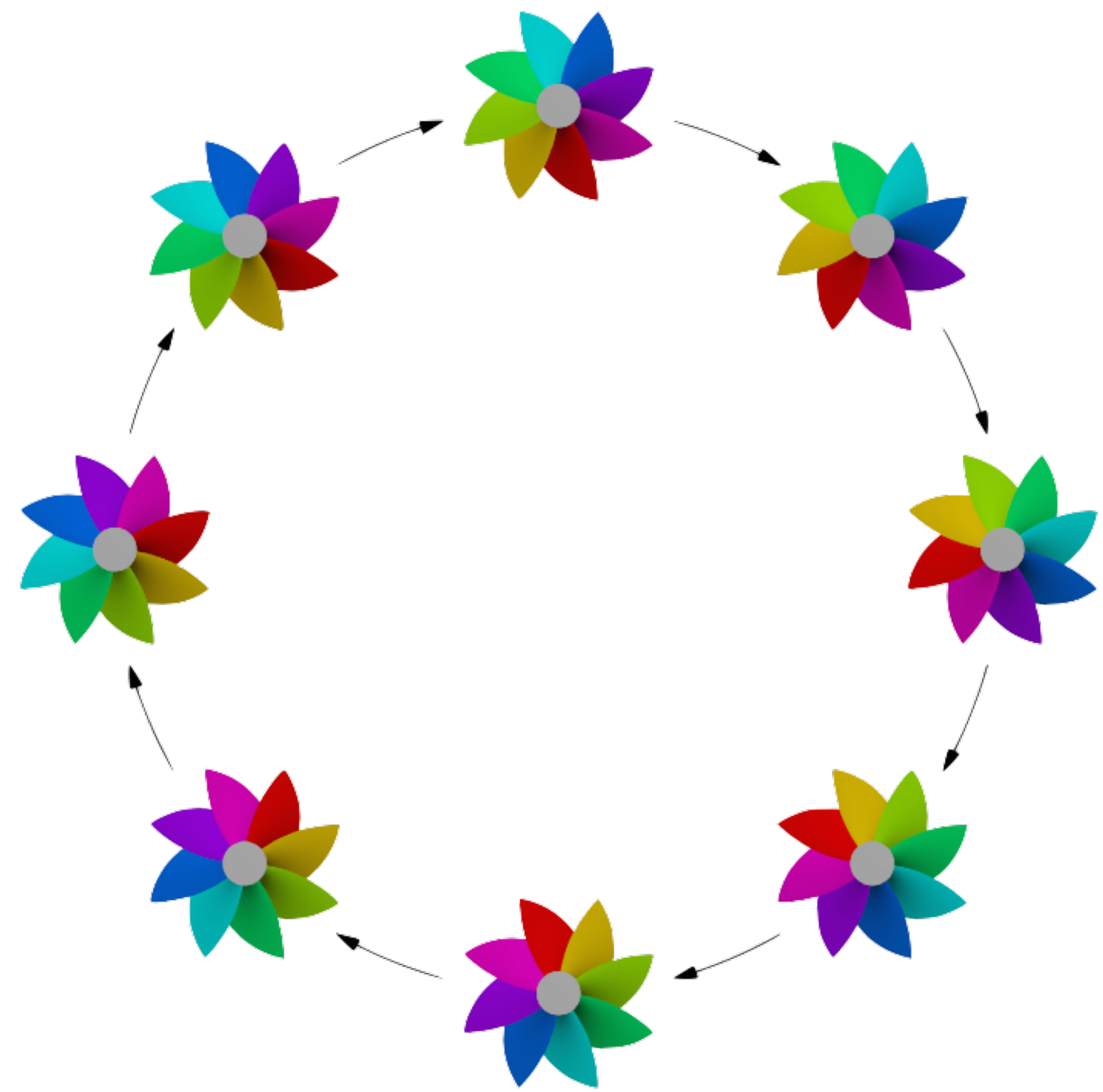


Nathan Carter, Bentley University

What Do Groups Look Like?

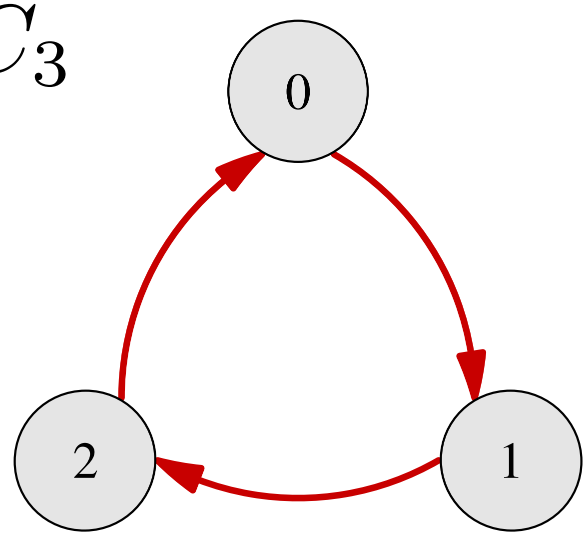
Cyclic Groups

Cyclic Groups

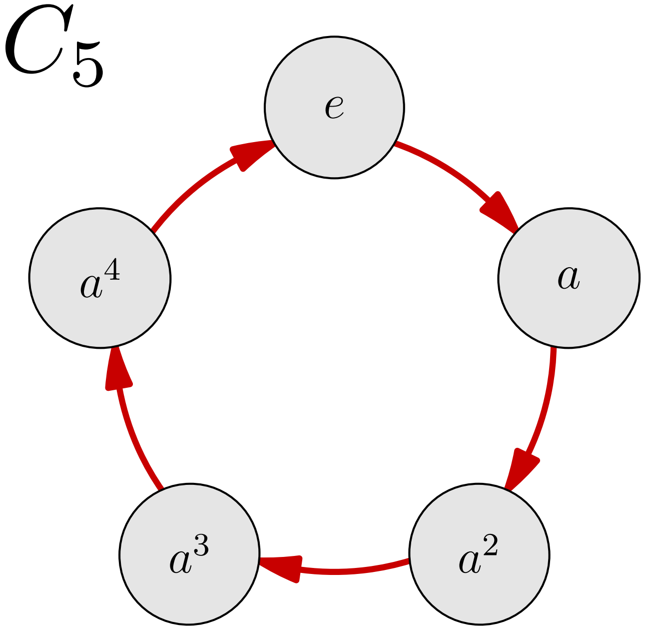


Cyclic Groups

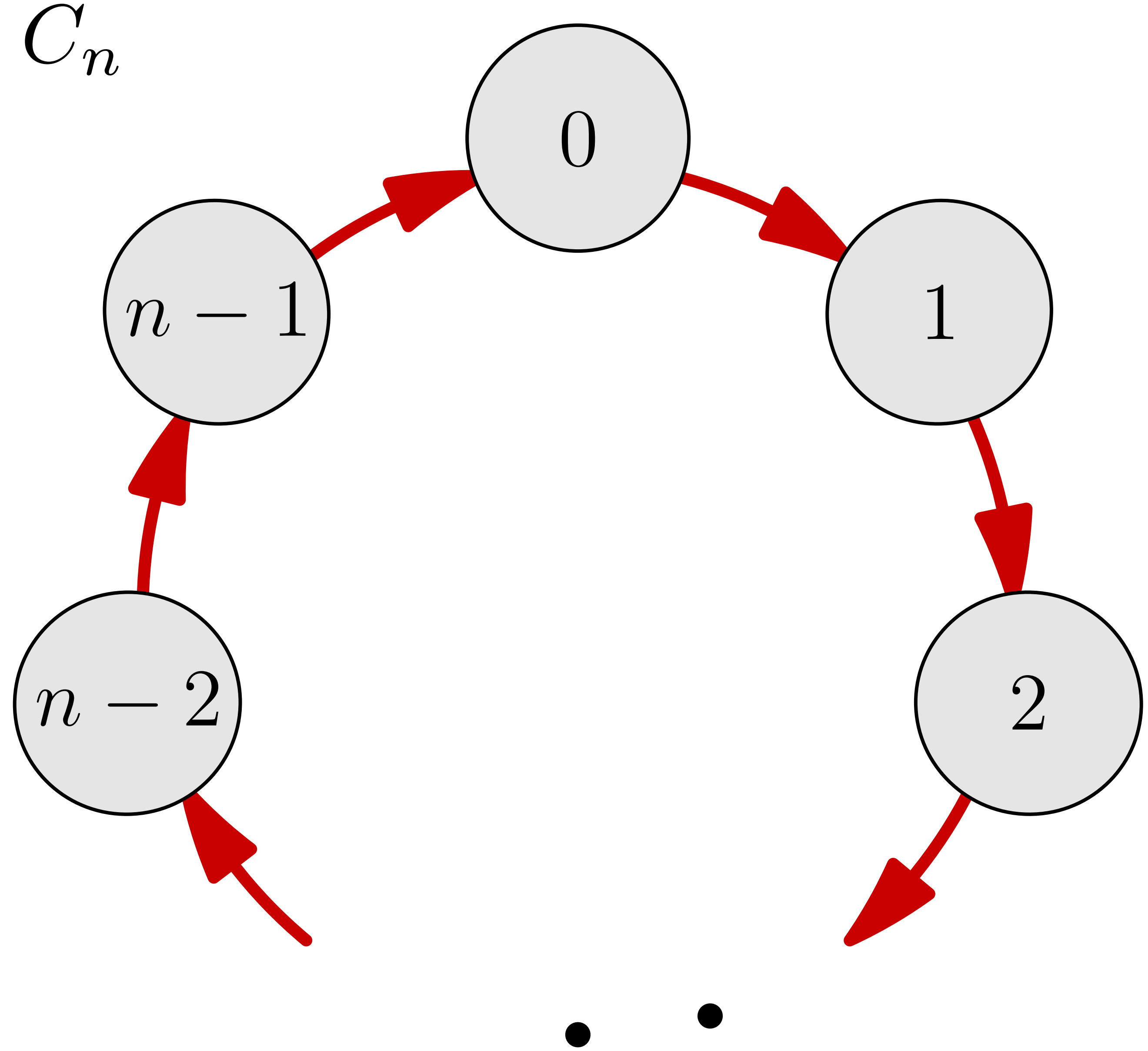
C_3



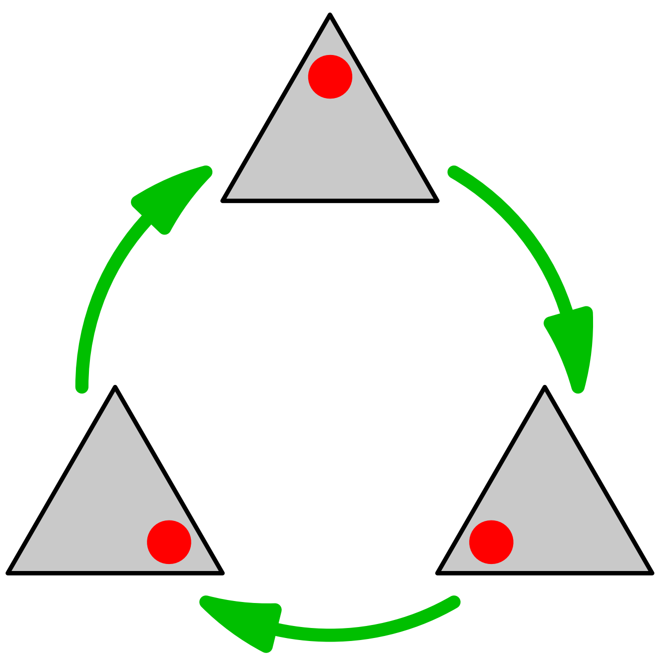
C_5



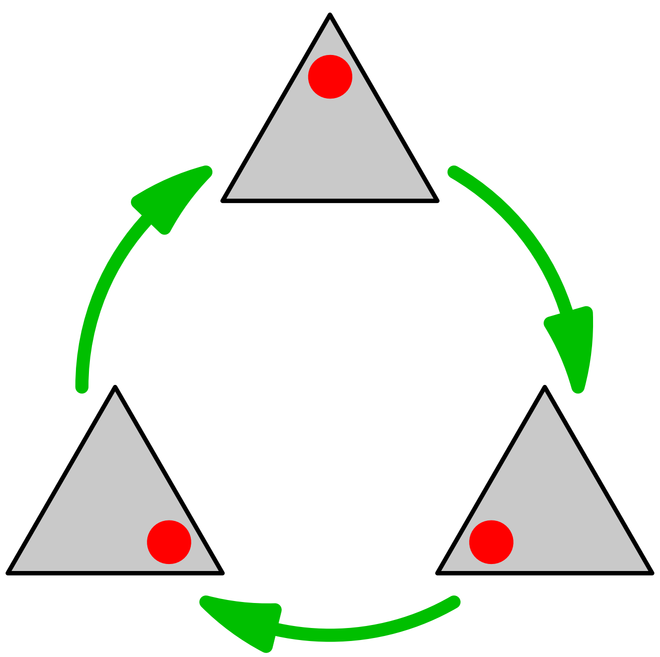
C_n

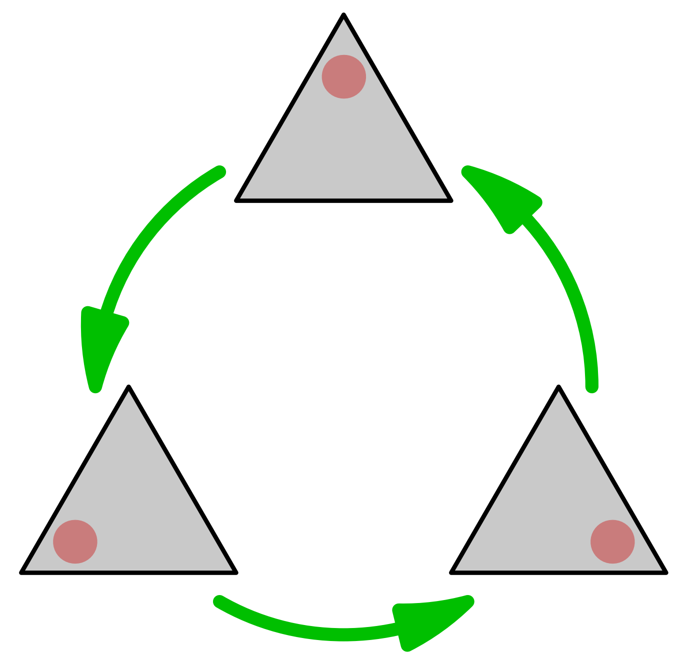


Dihedral Groups

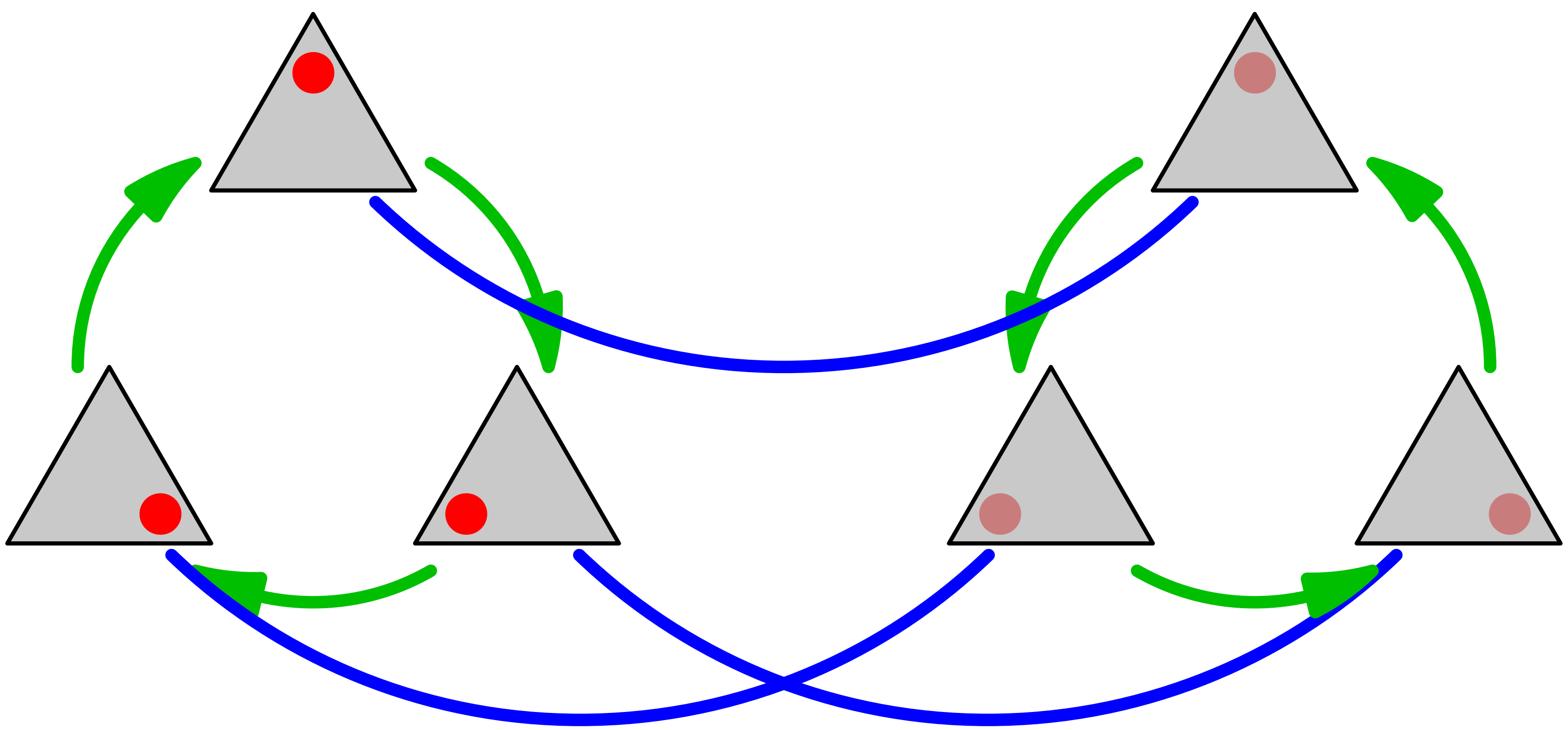


Dihedral Groups

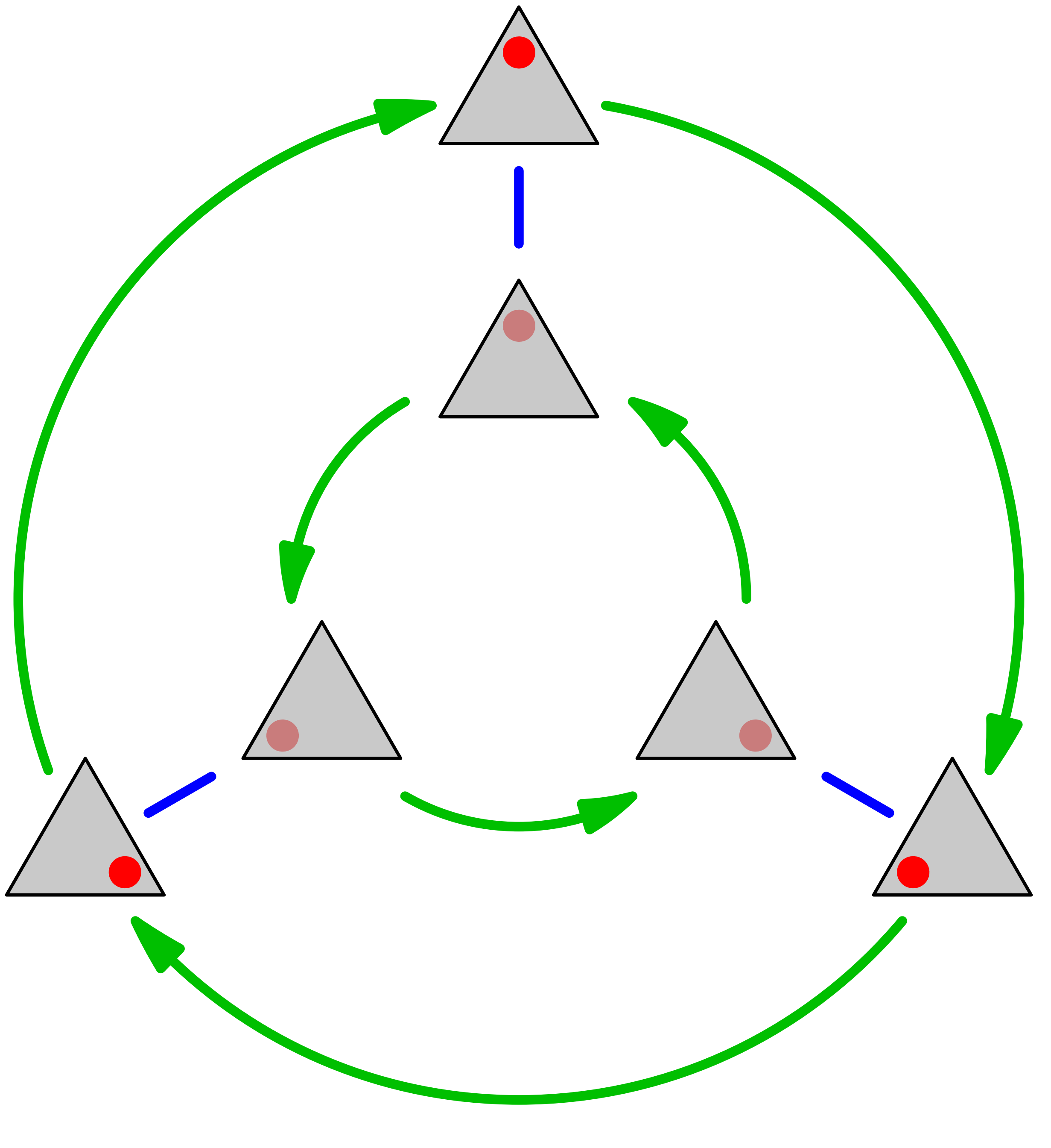




Dihedral Groups

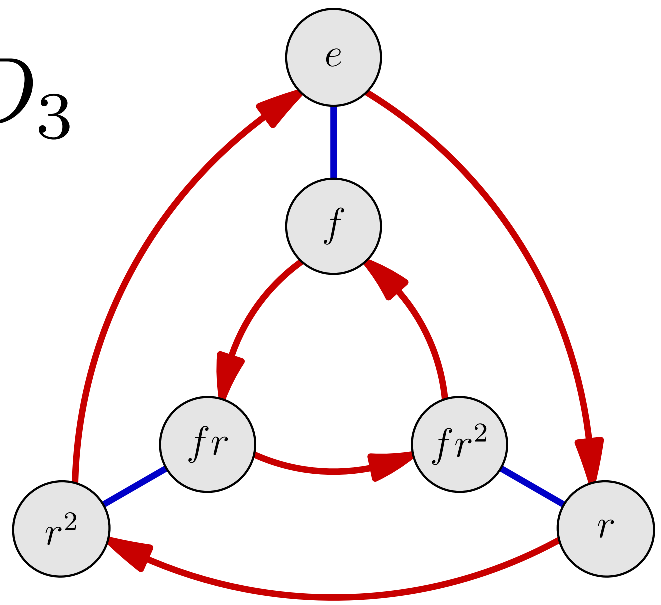


Dihedral Groups

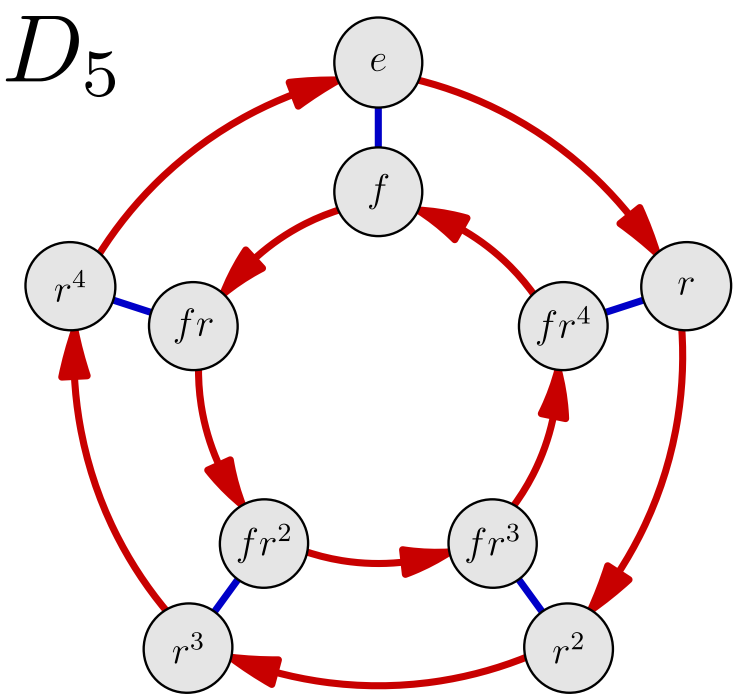


Dihedral Groups

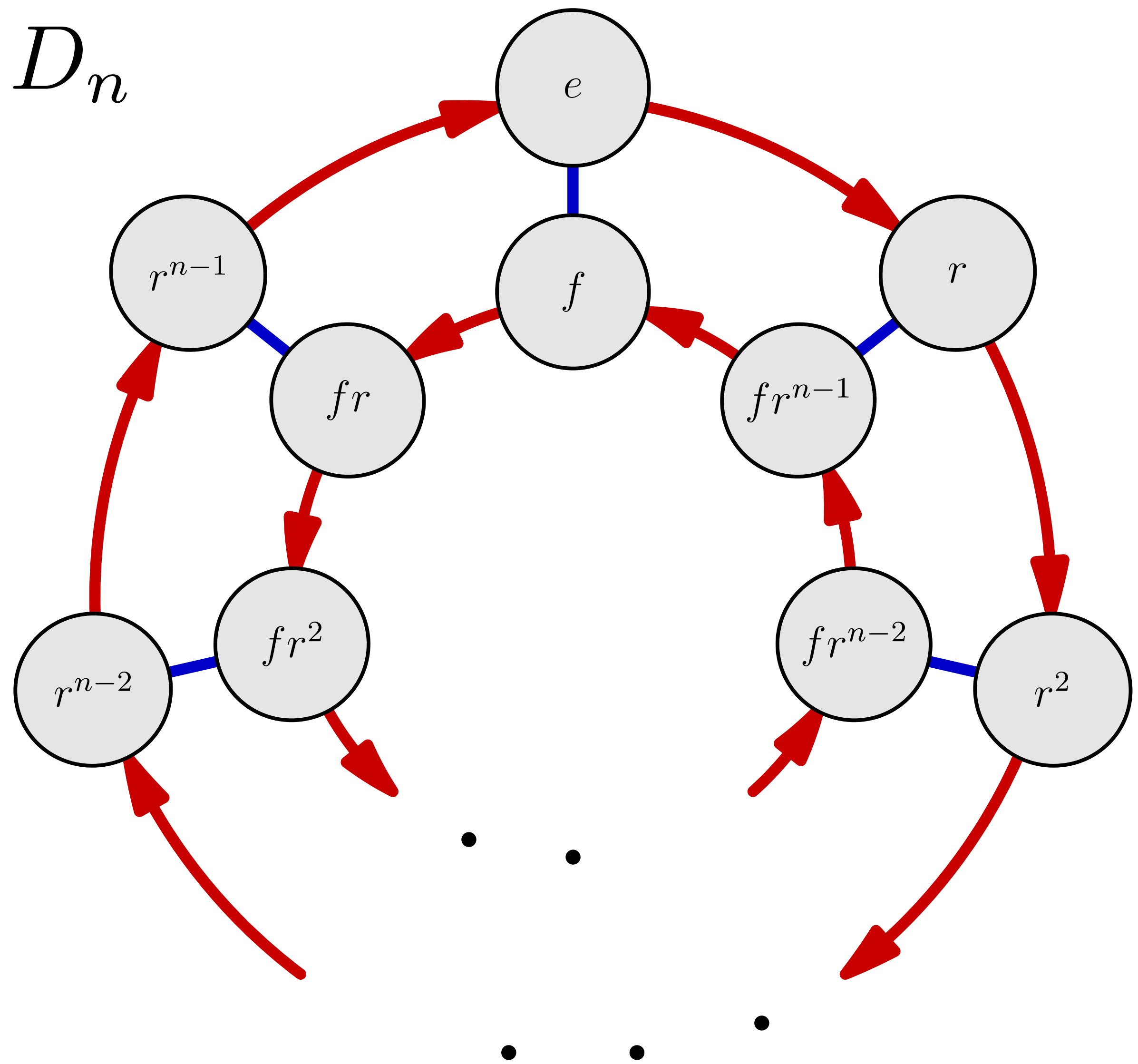
D_3



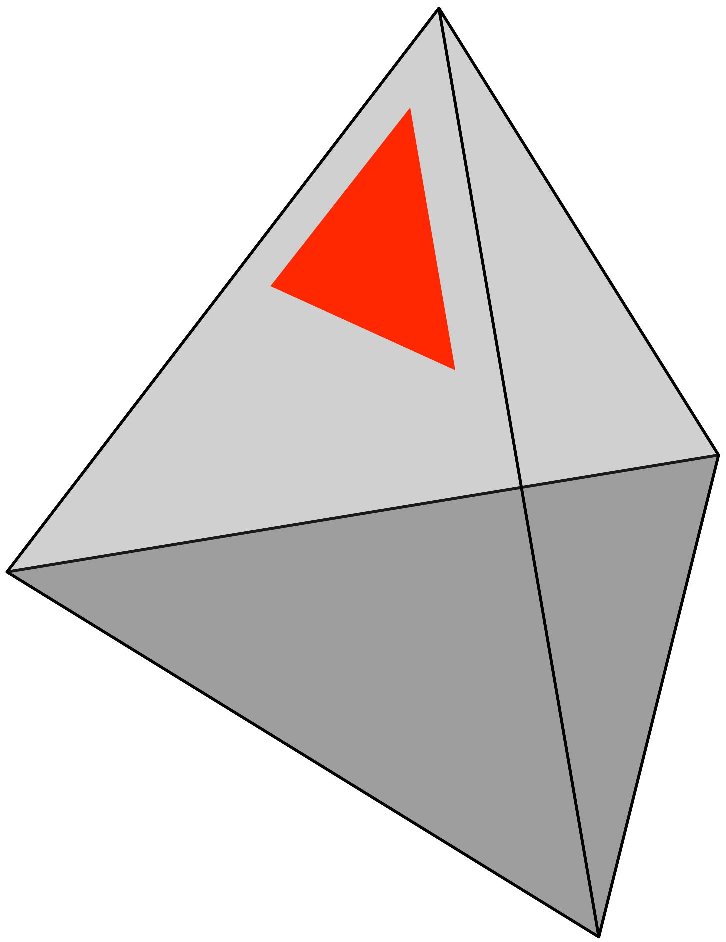
D_5



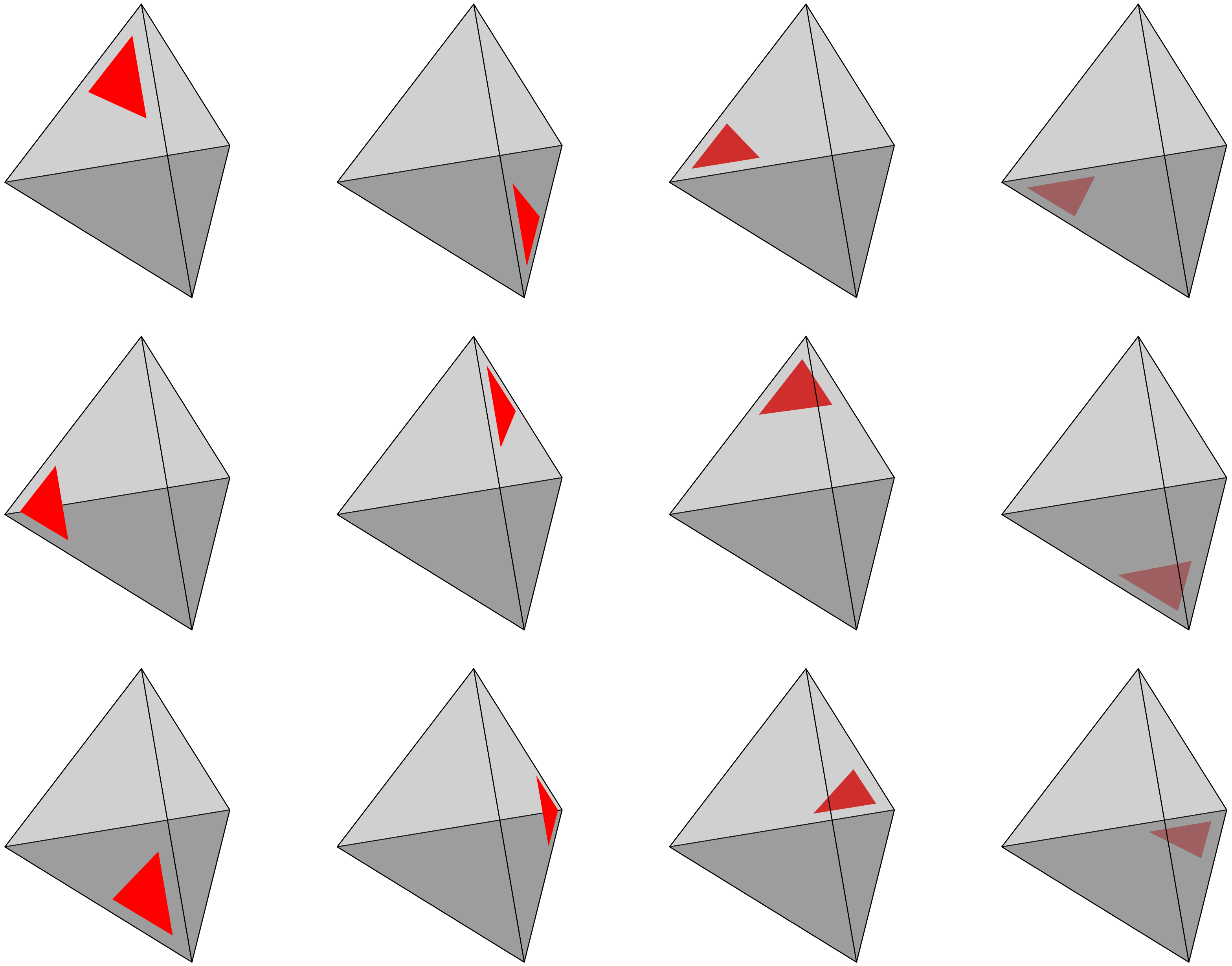
D_n



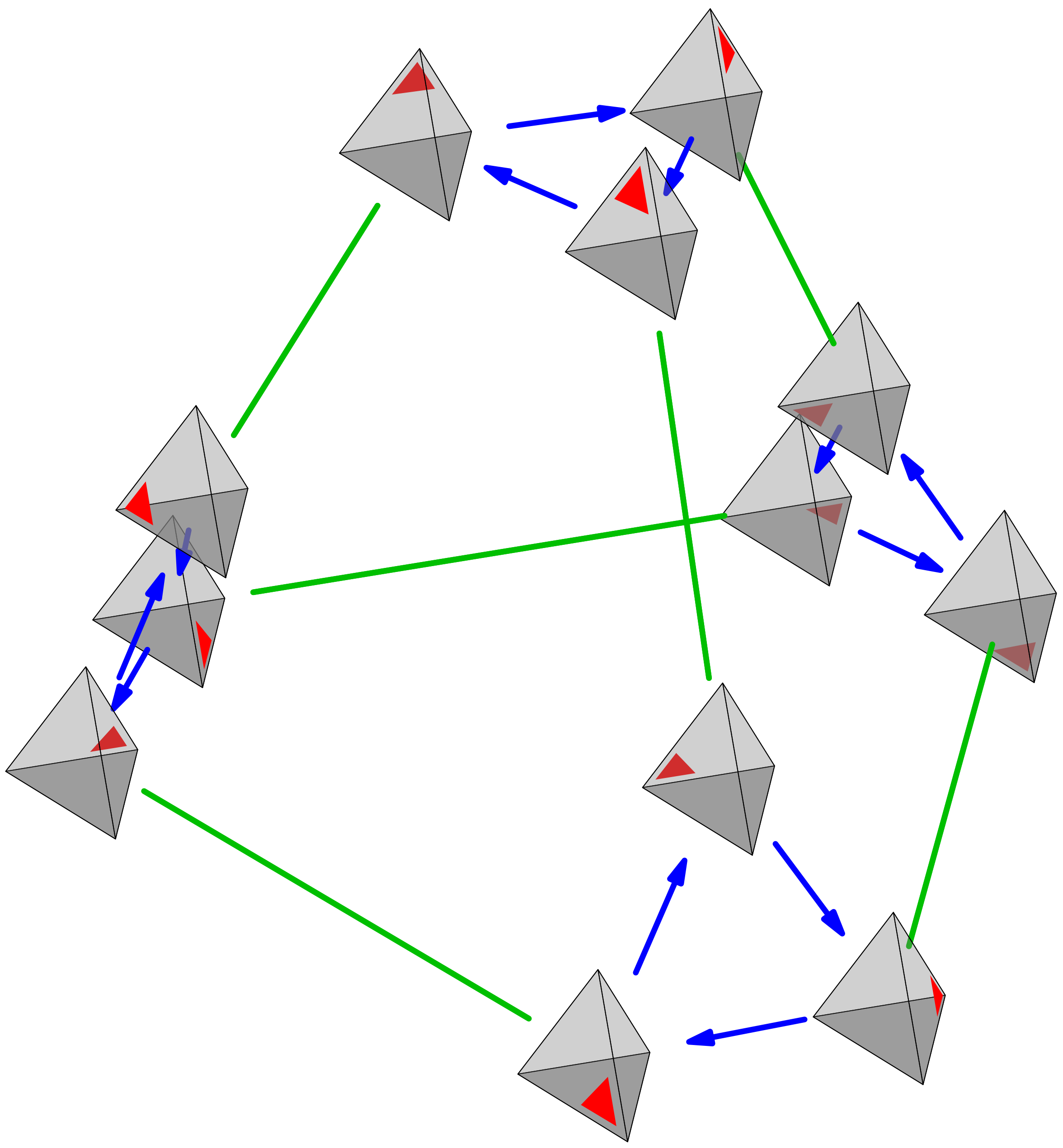
Symmetric and Alternating Groups



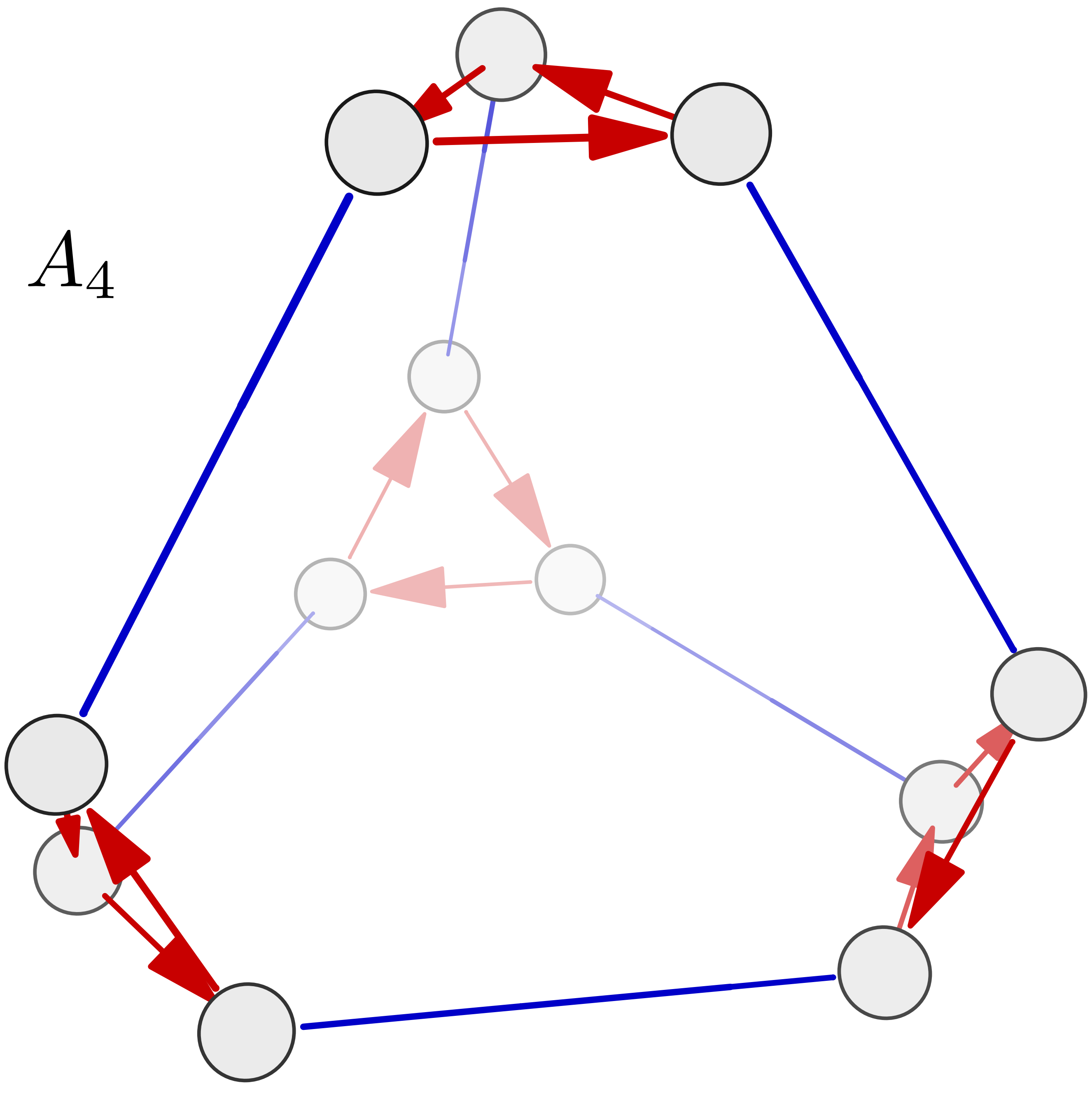
Symmetric and Alternating Groups



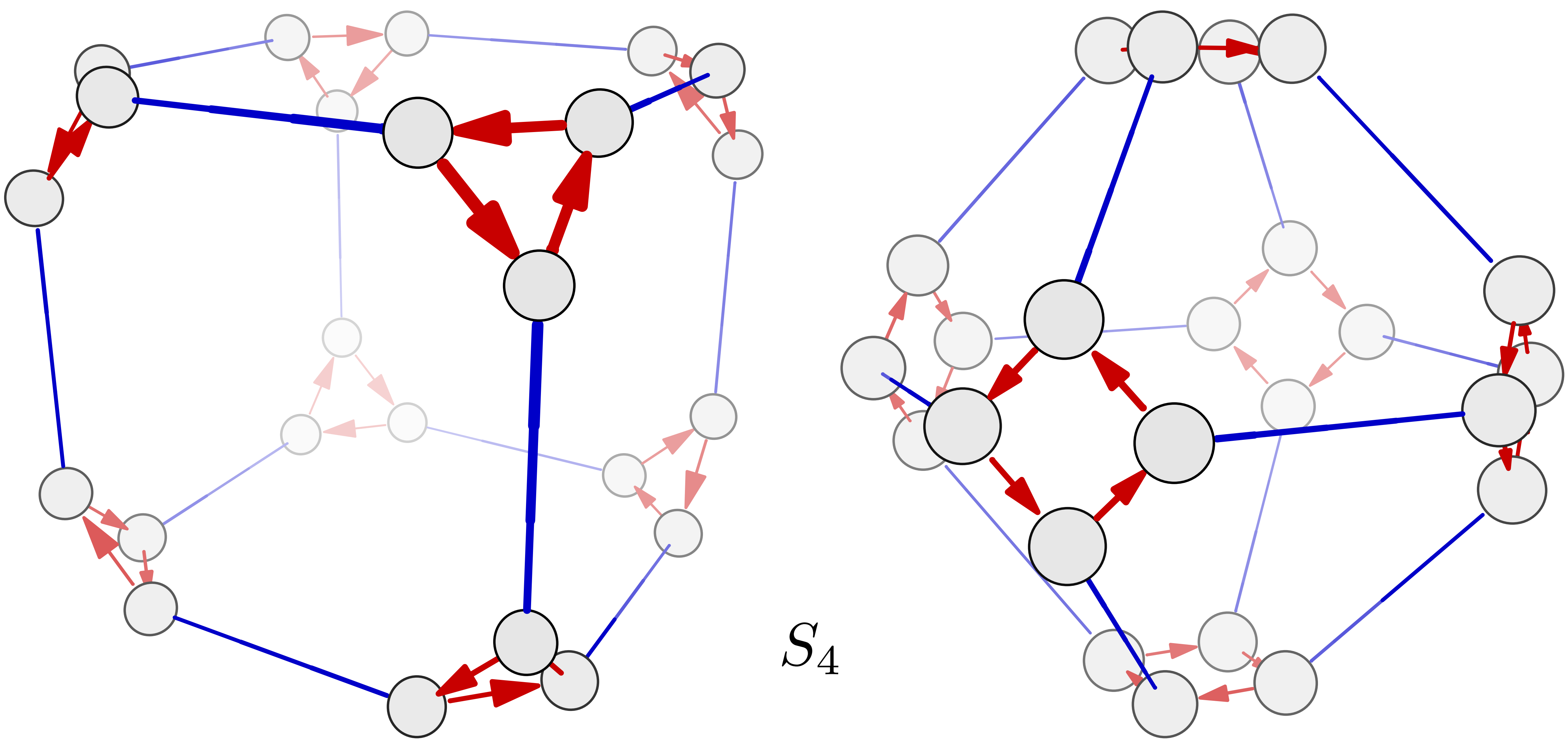
Symmetric and Alternating Groups



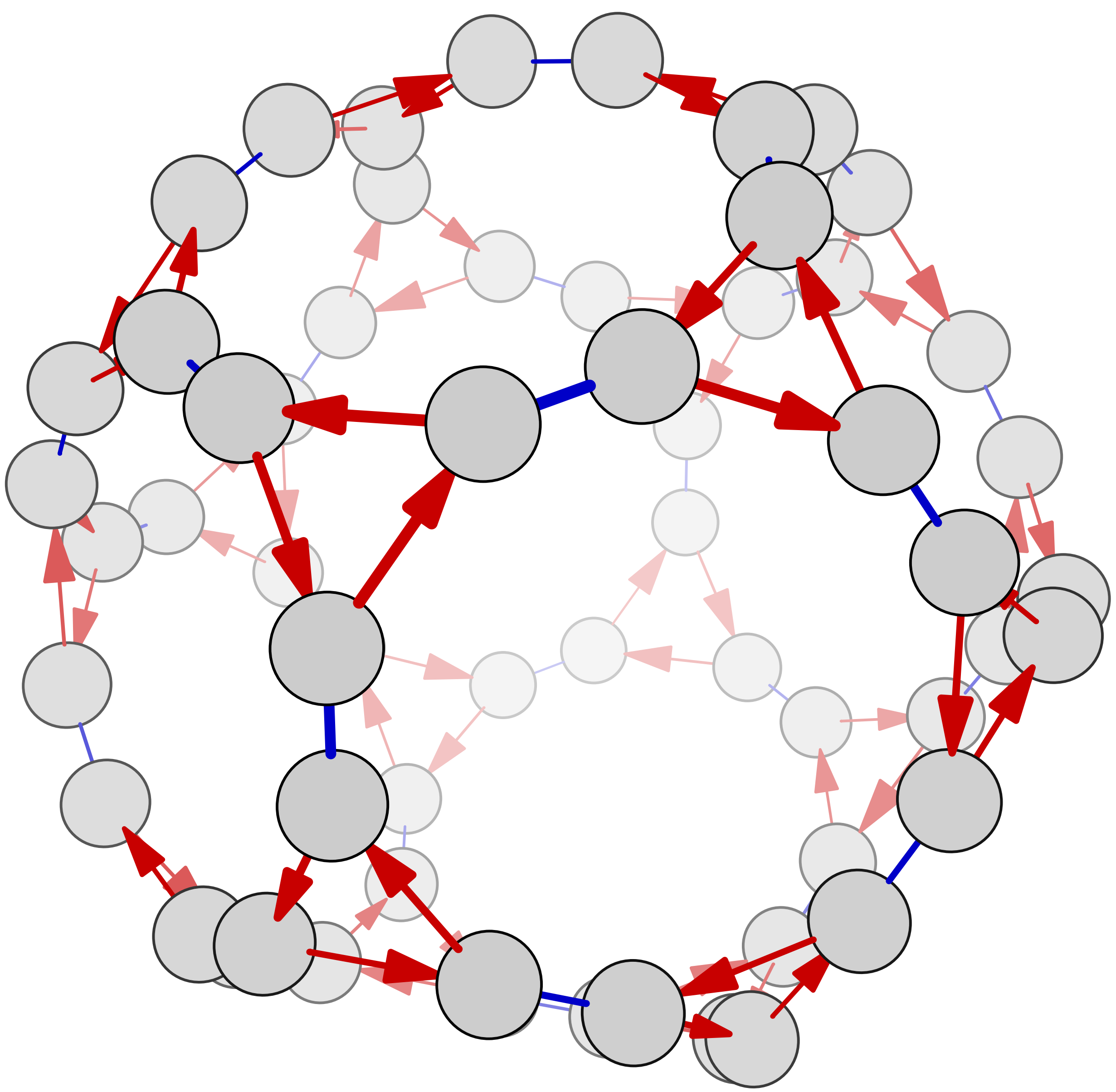
Symmetric and Alternating Groups



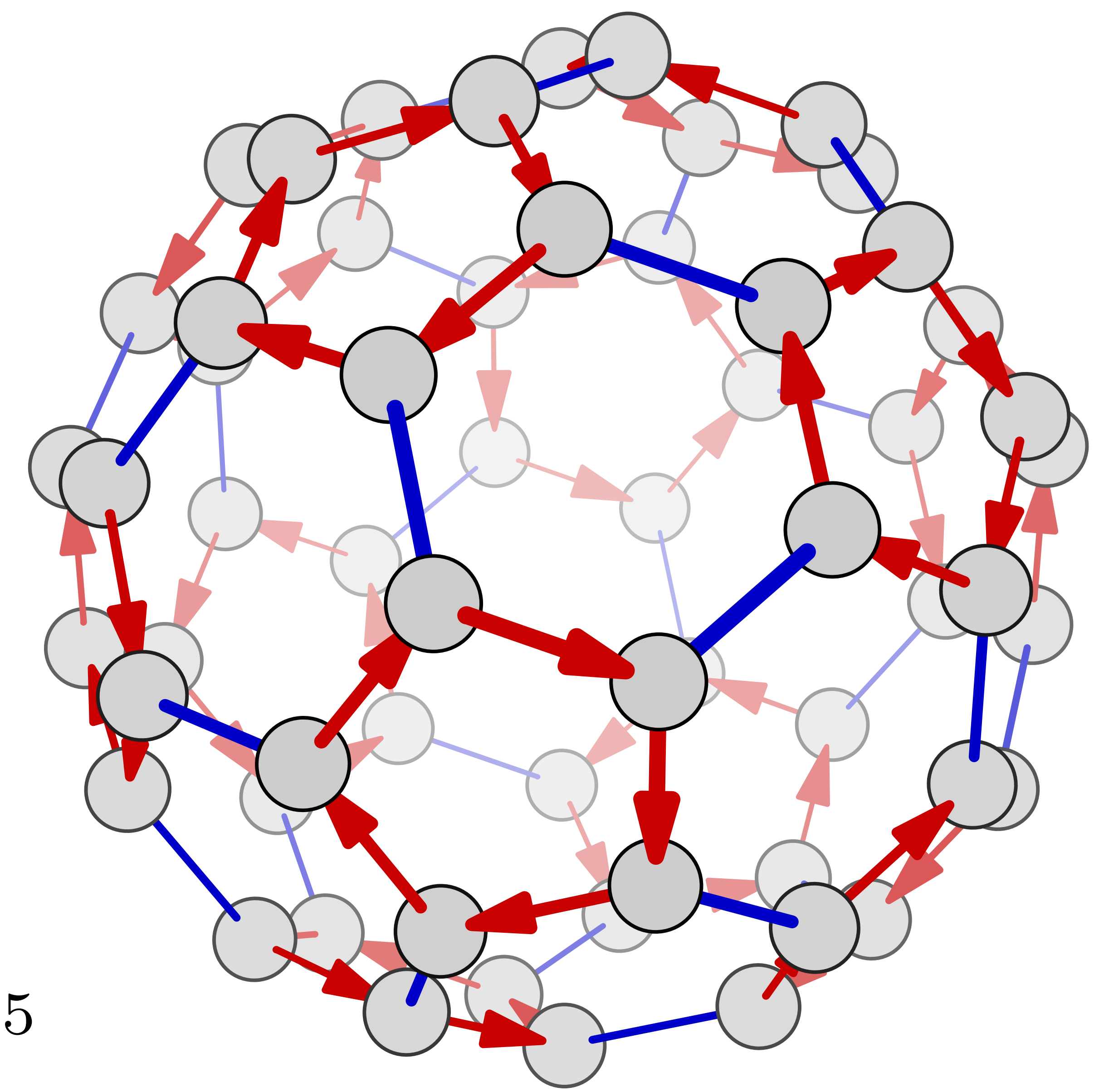
Symmetric and Alternating Groups



Symmetric and Alternating Groups

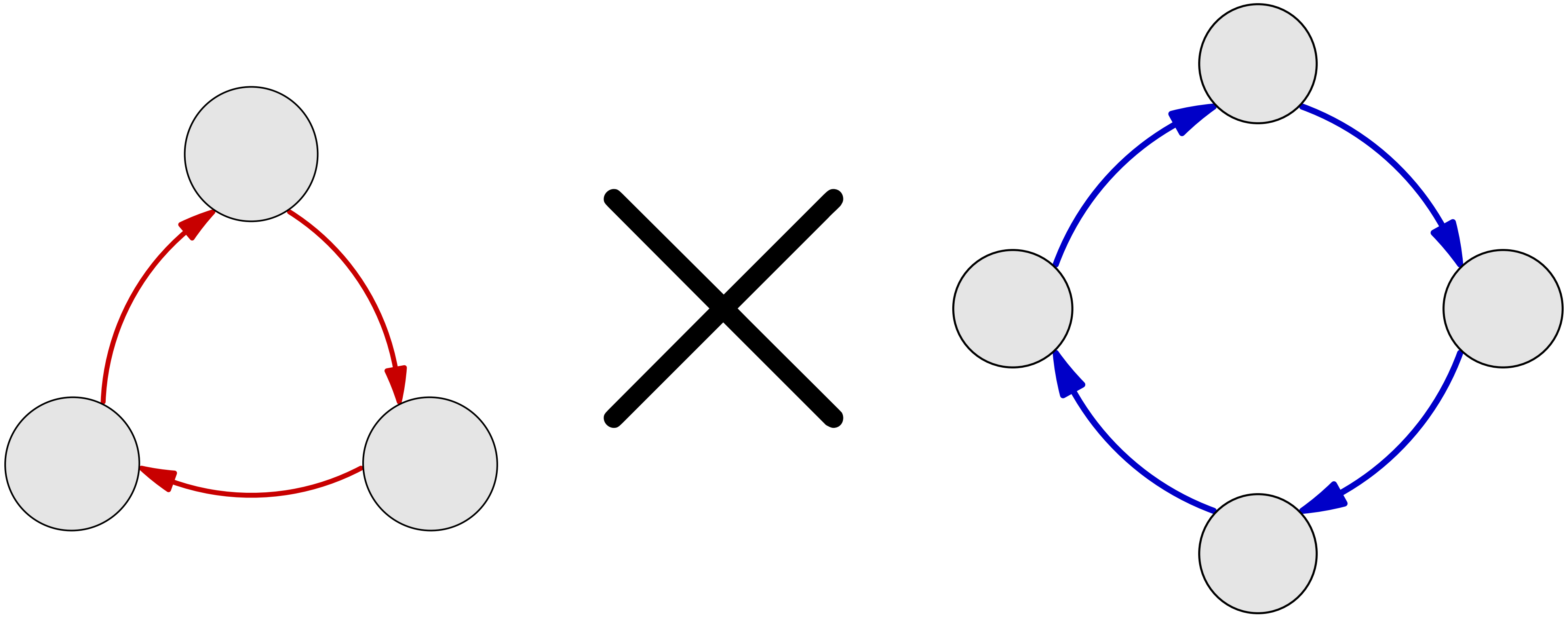


A_5



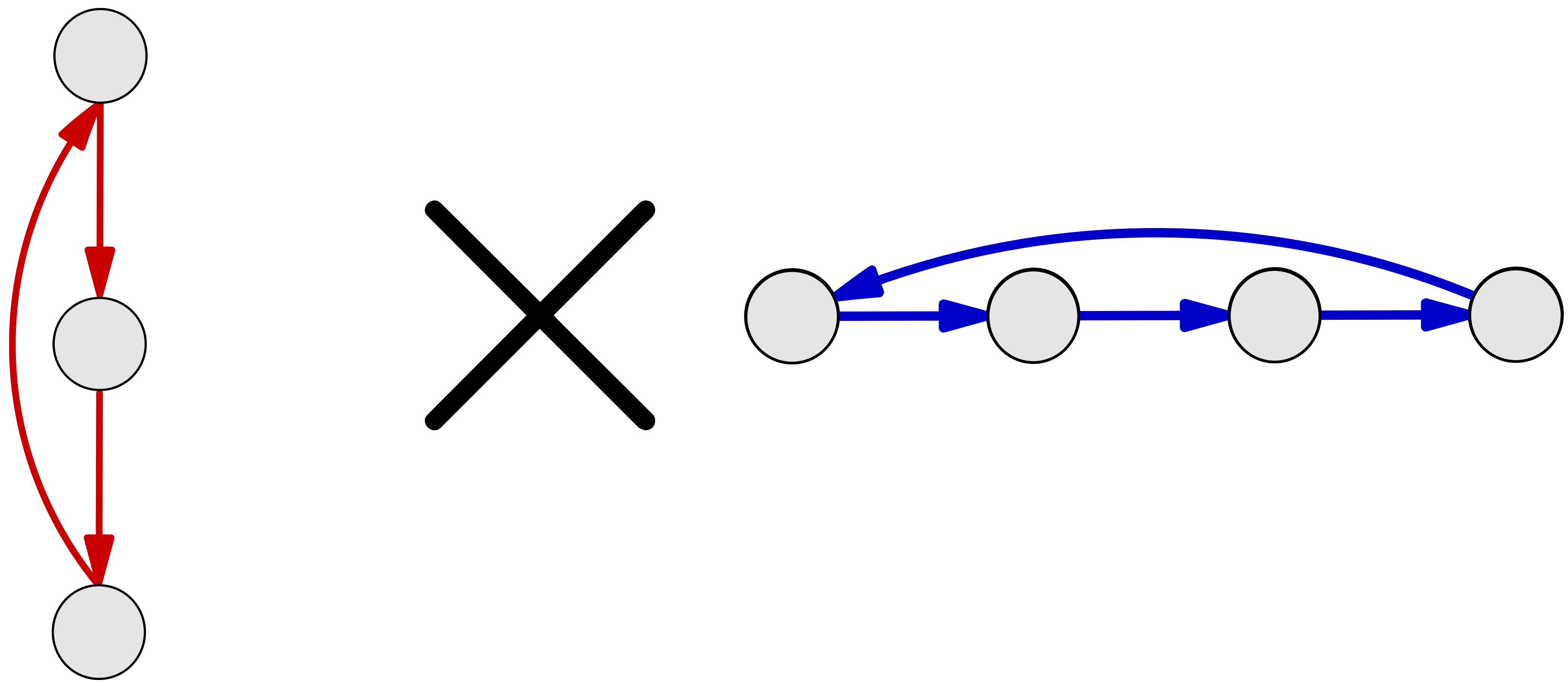
How big can groups get?

Direct Products

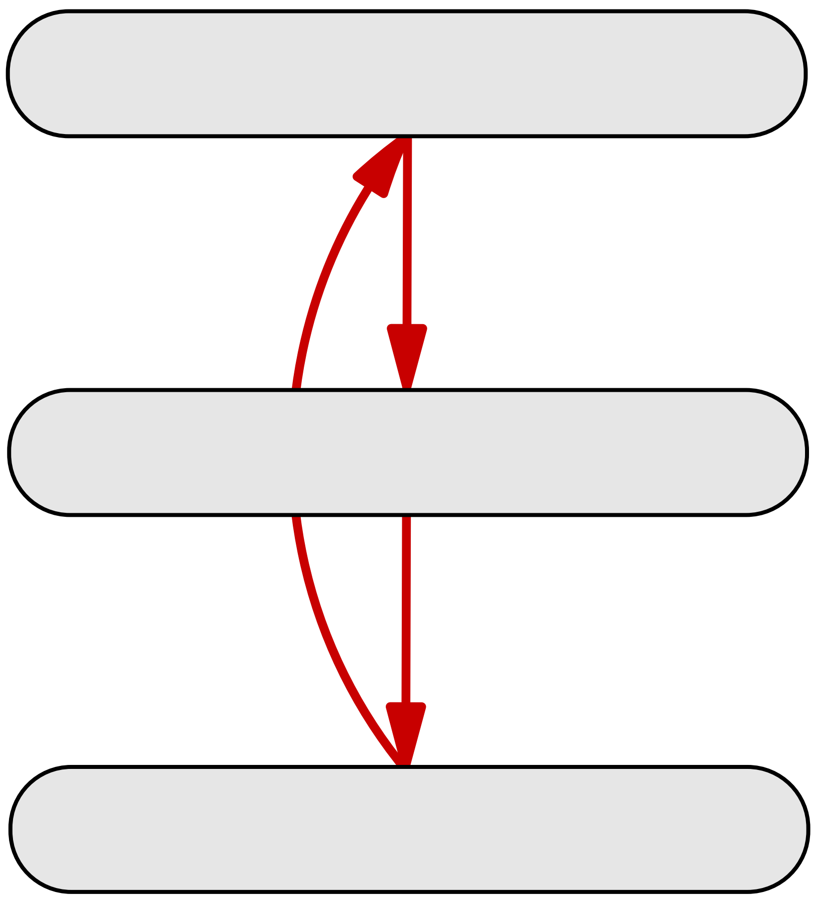


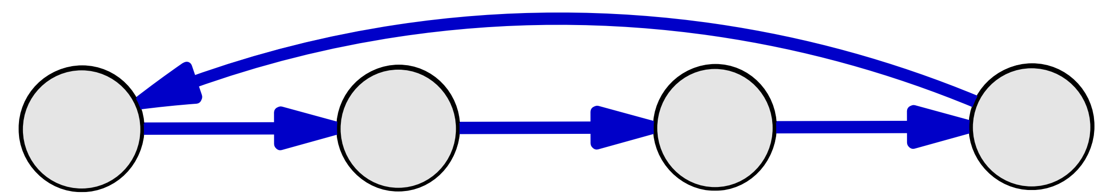
C_3 $\times$ C_4

Direct Products

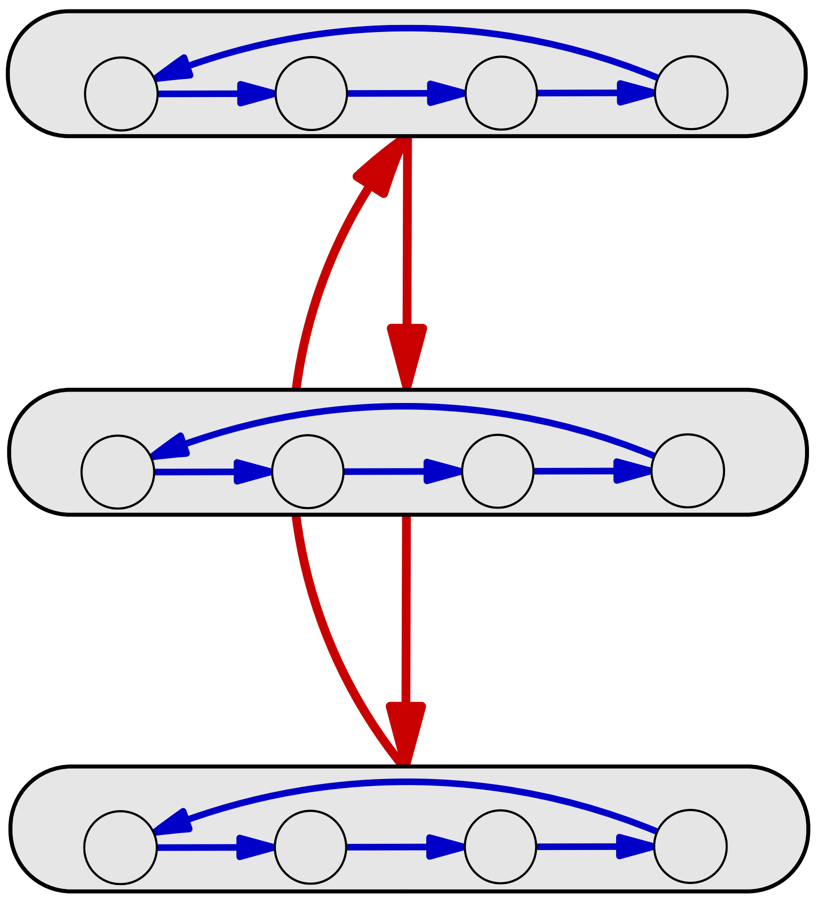


Direct Products

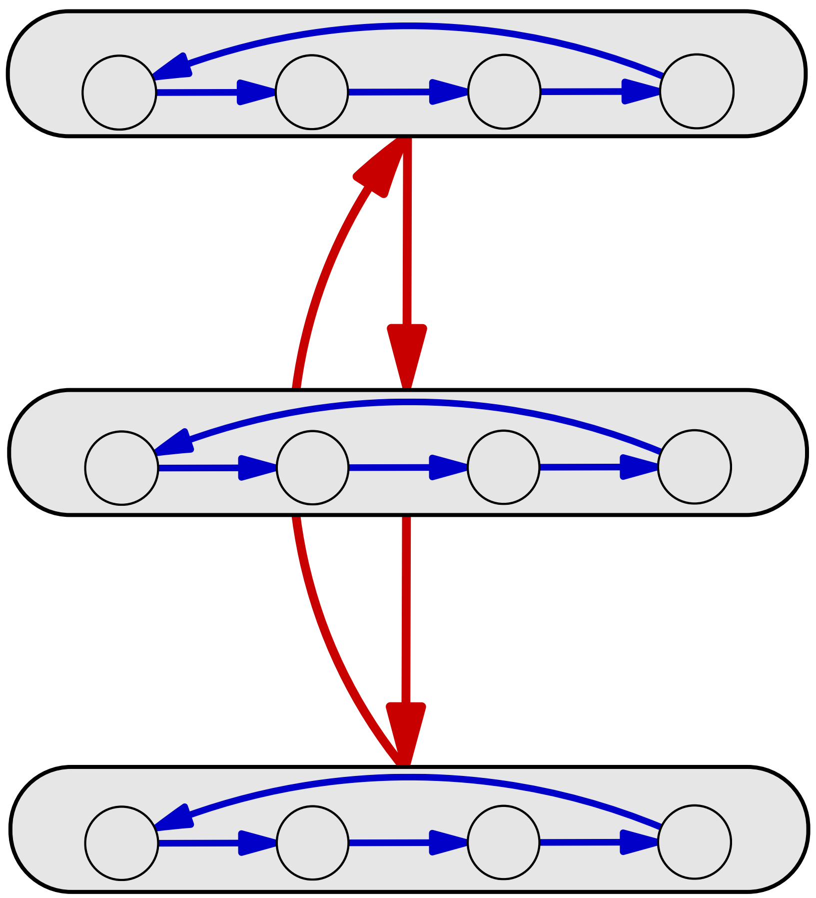




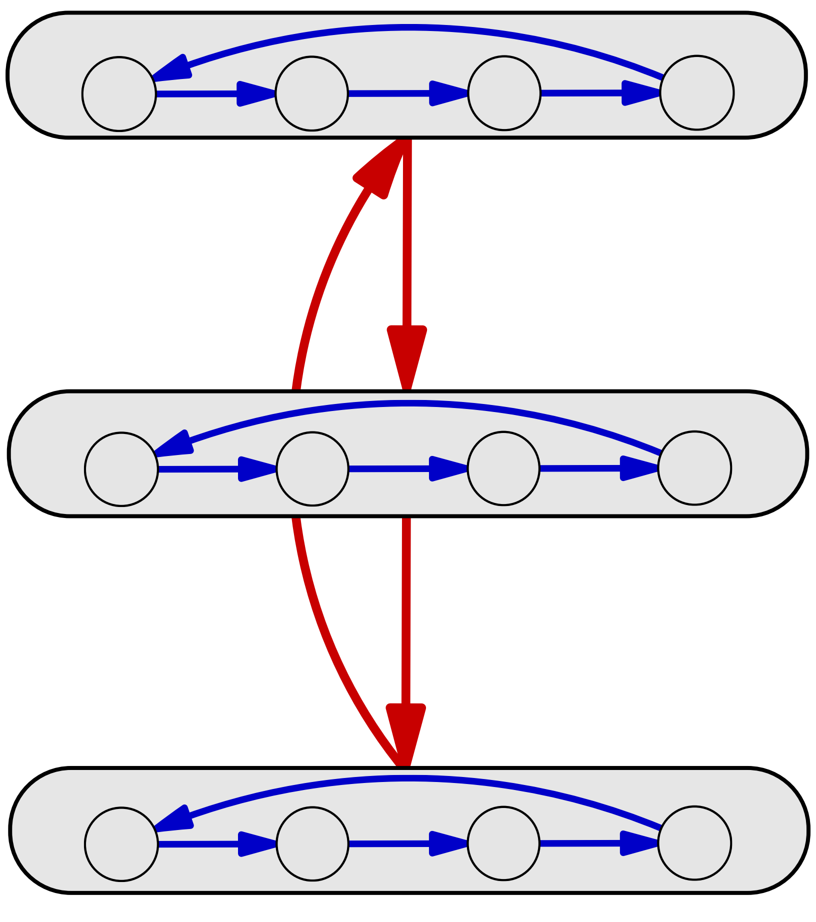
Direct Products



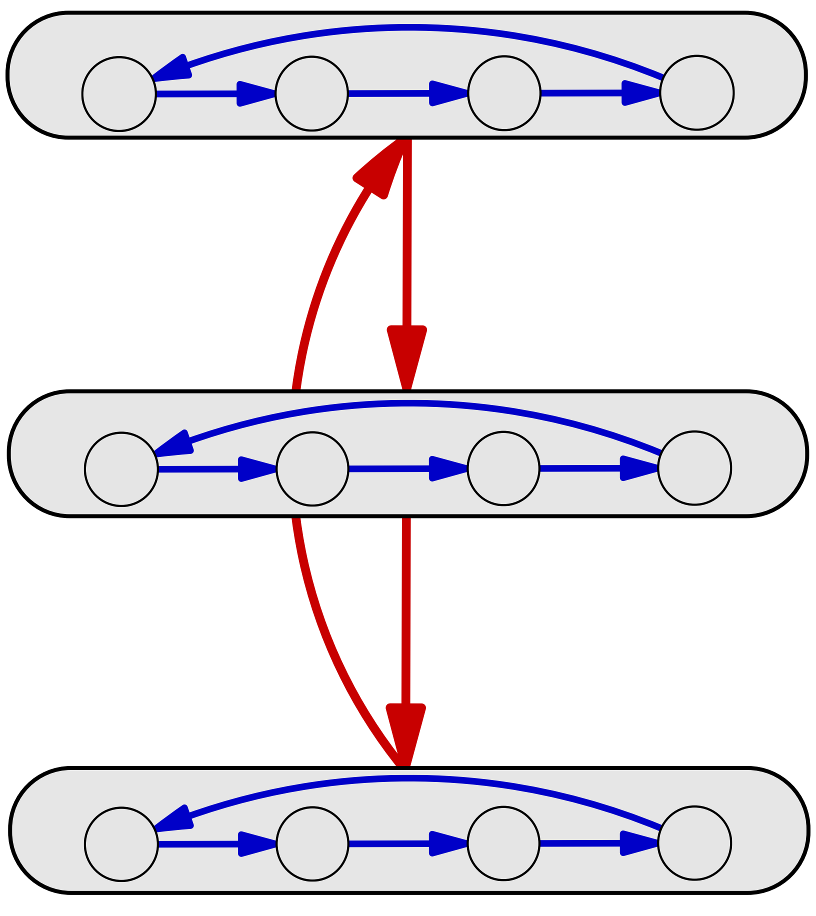
Direct Products



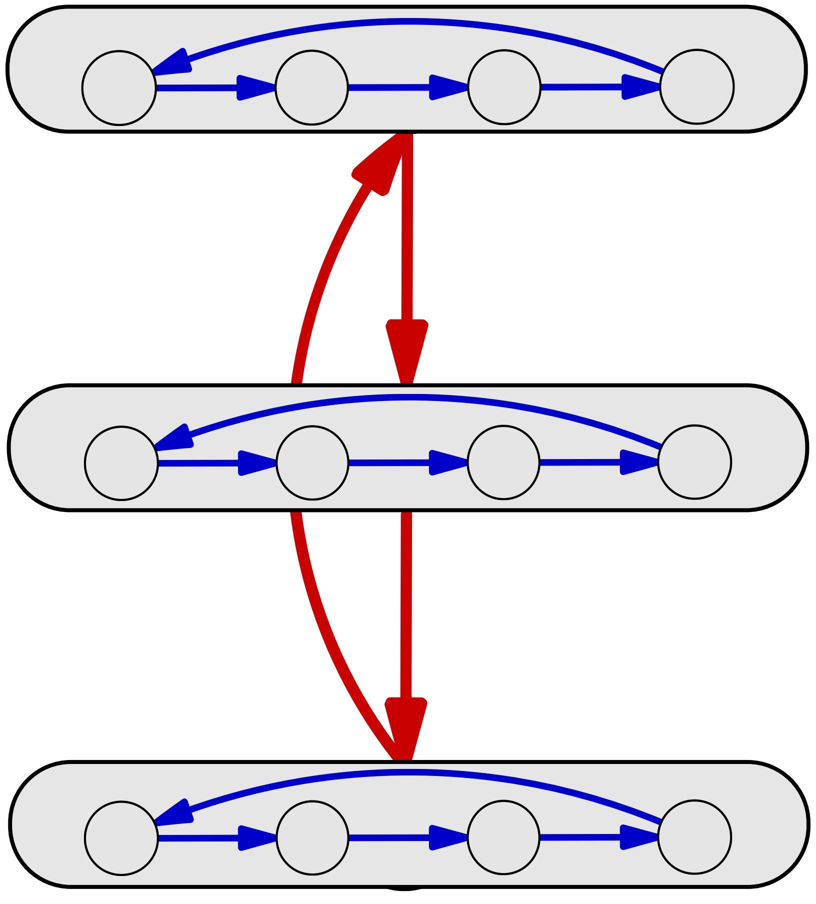
Direct Products



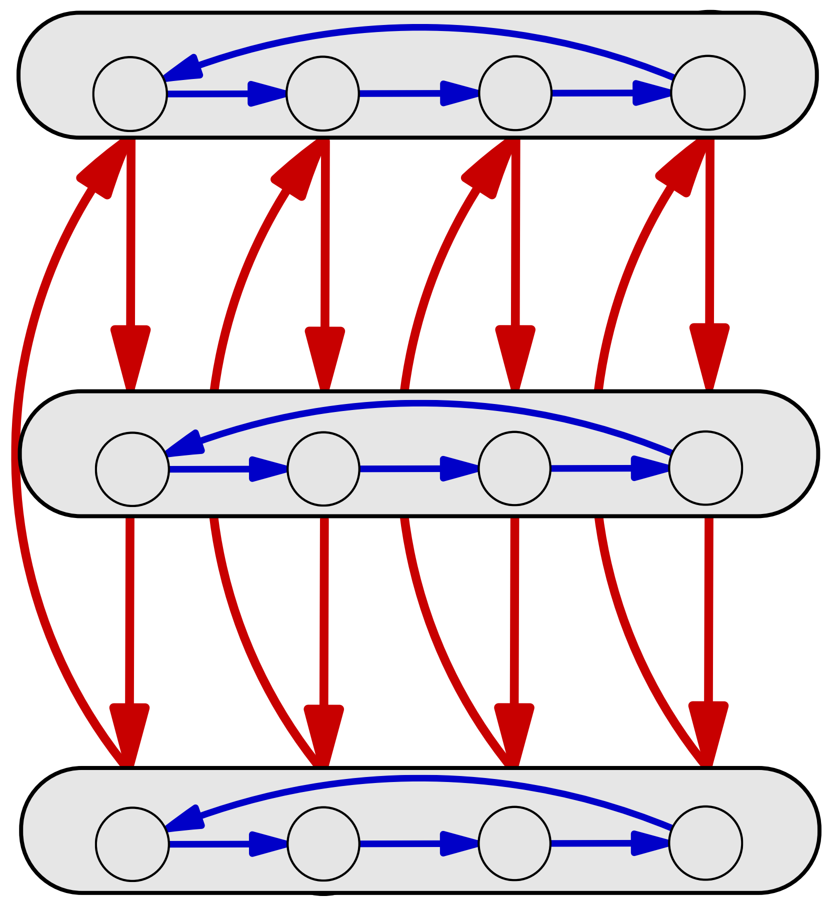
Direct Products



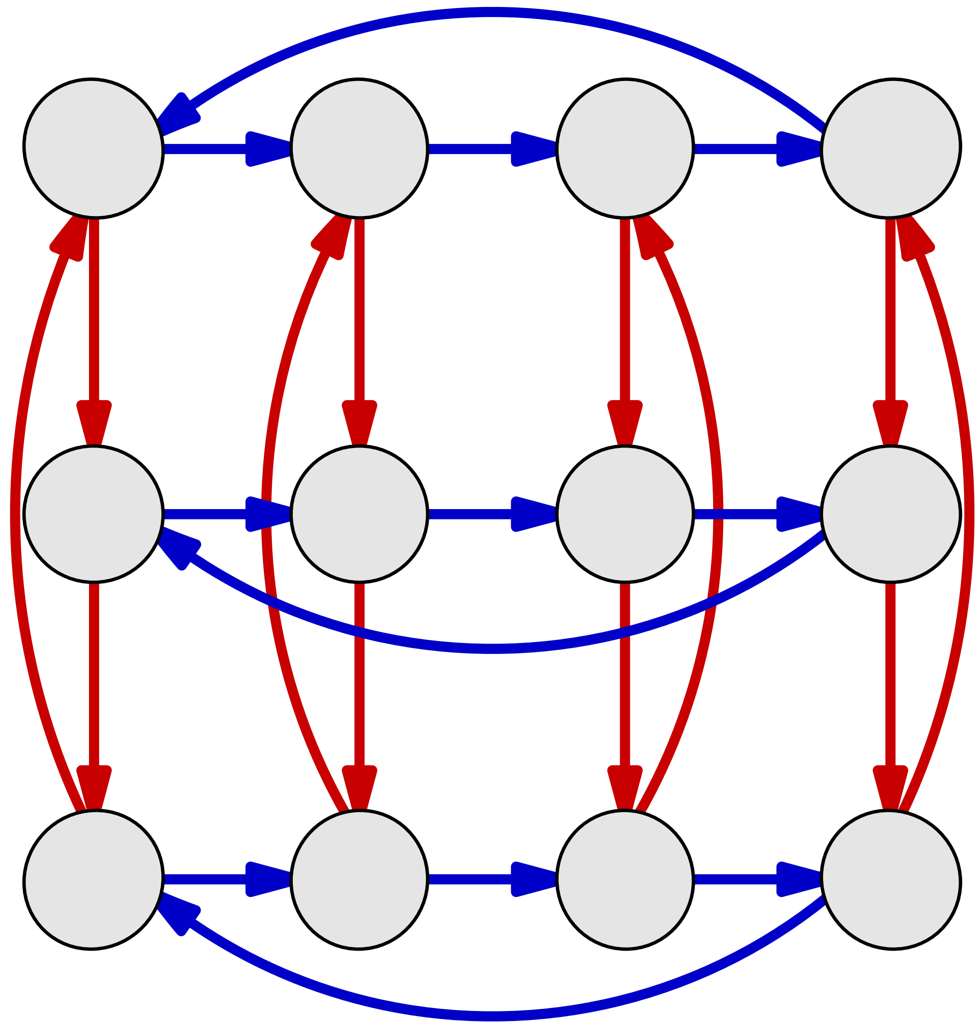
Direct Products



Direct Products



Direct Products



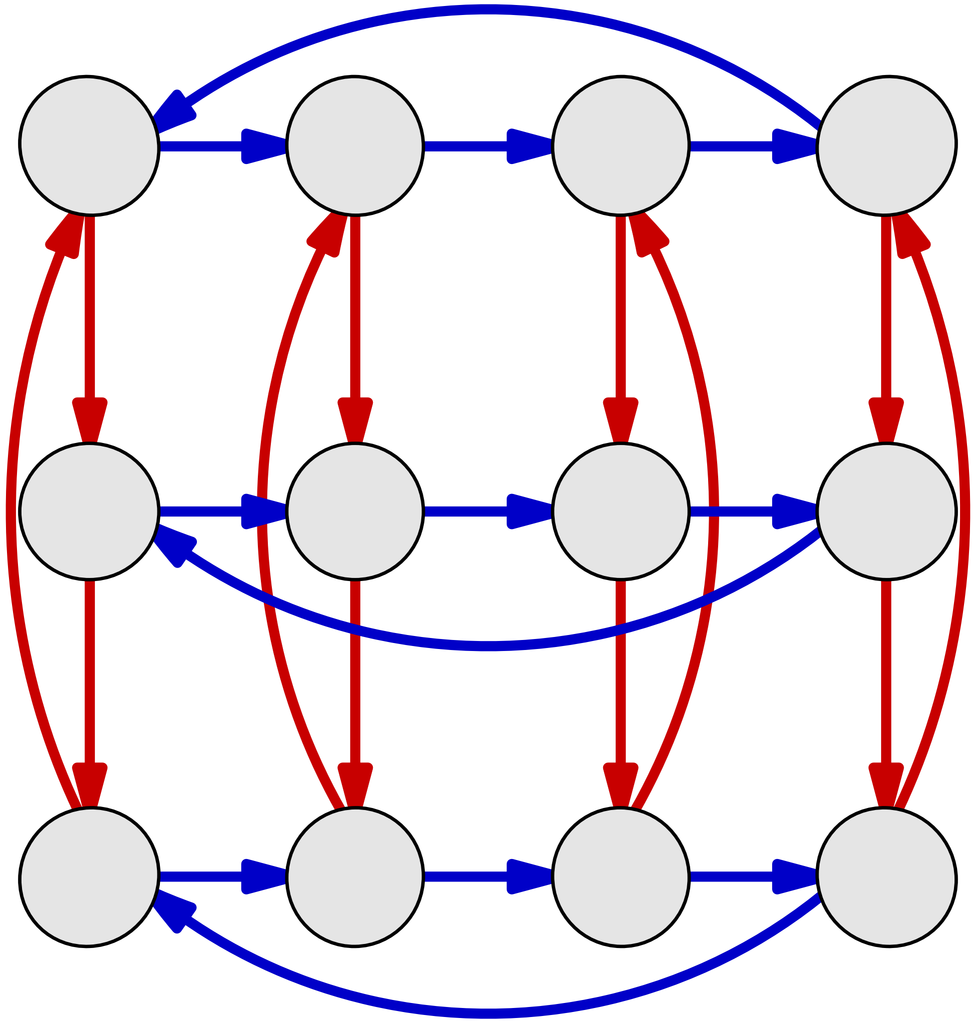
$C_3 \times C_4$

Are there non-Direct Products?

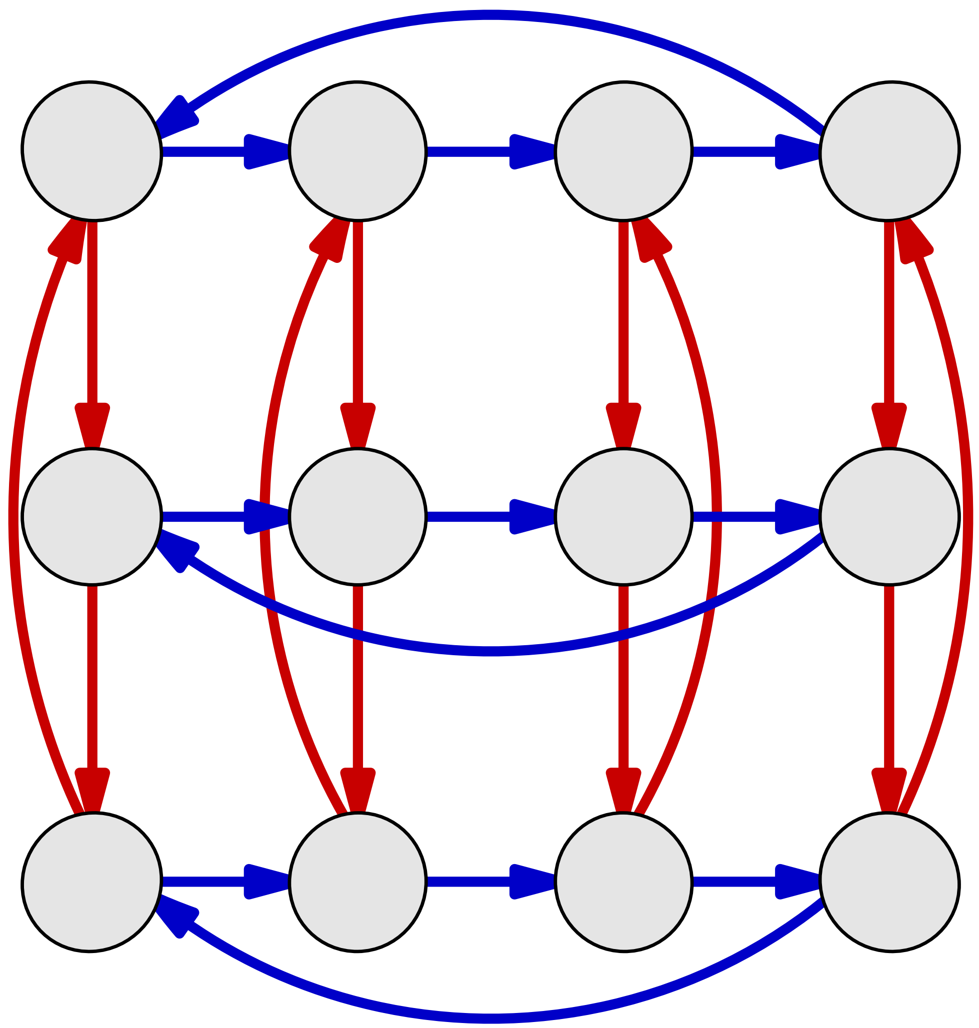
Are there non-Direct Products?

Just wait…

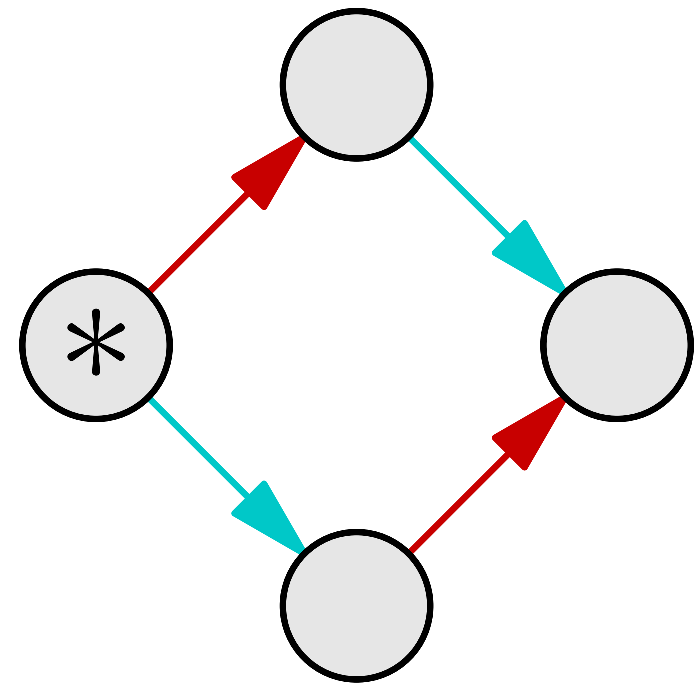
Are all groups as boring as that one?



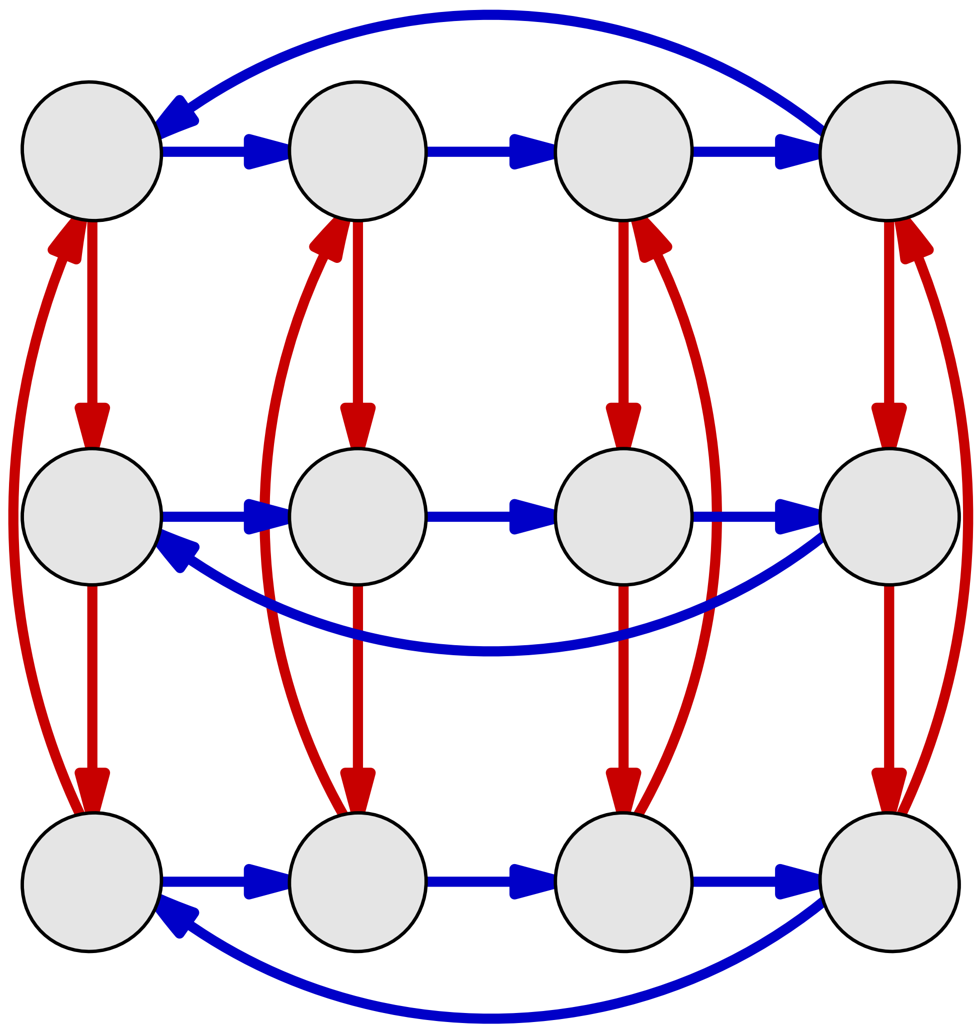
$C_3 \times C_4$



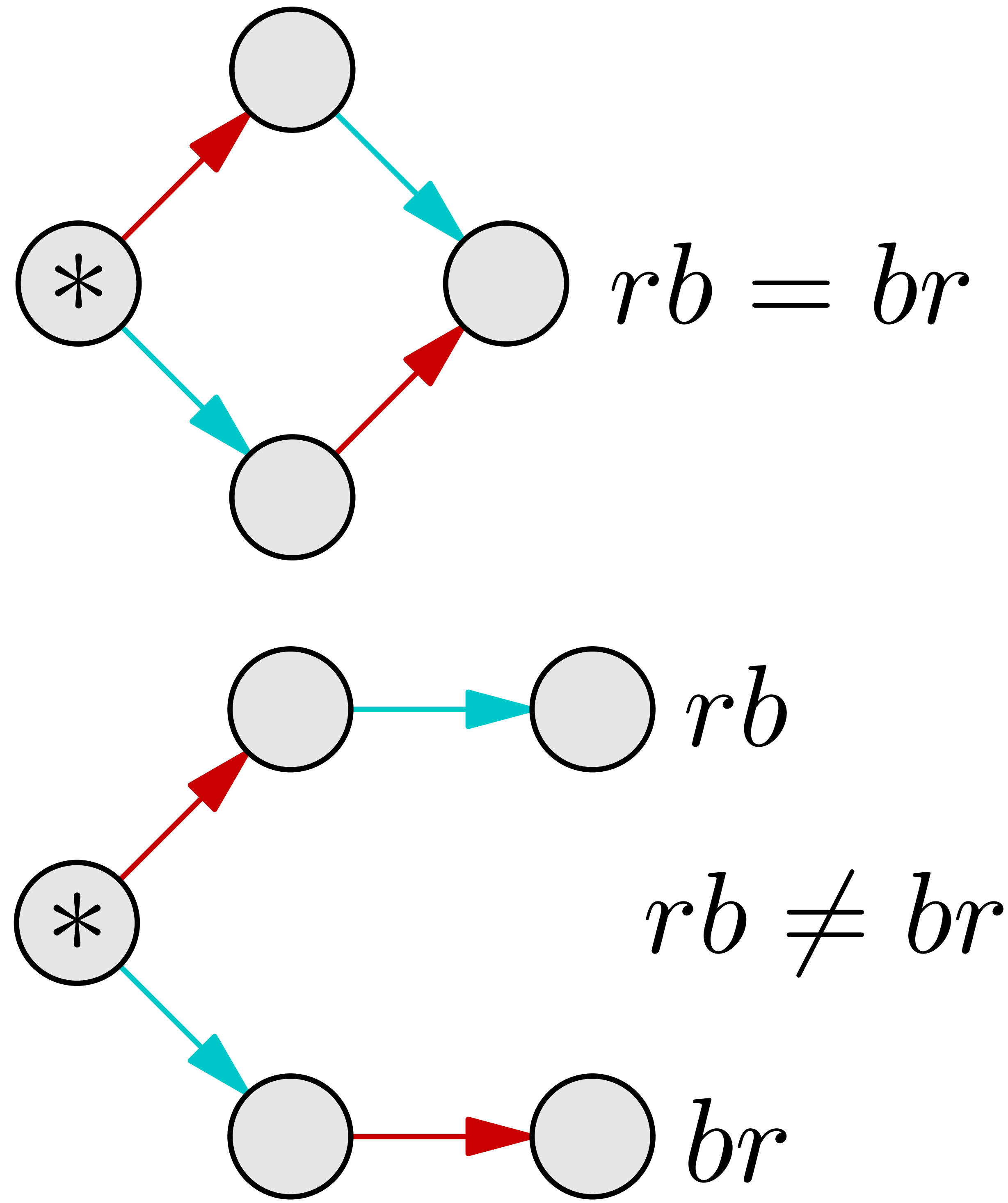
$C_3 \times C_4$



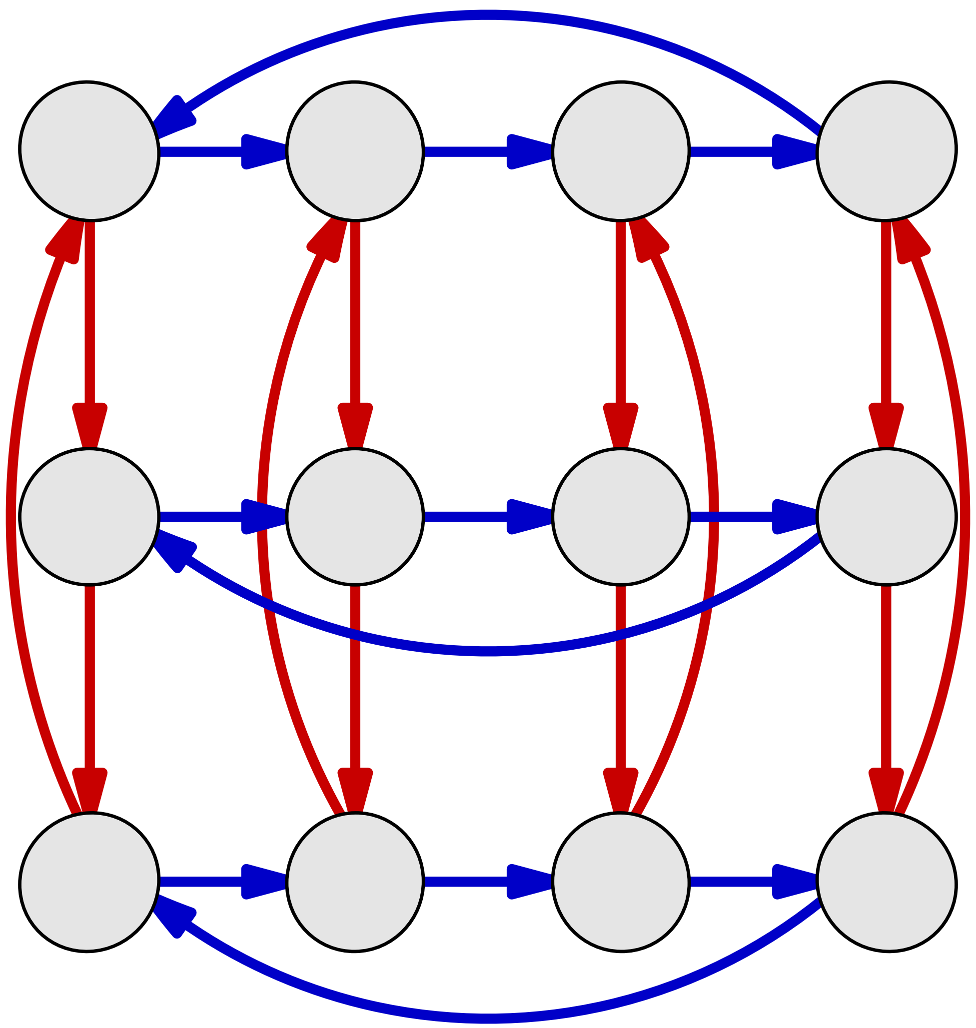
$rb = br$



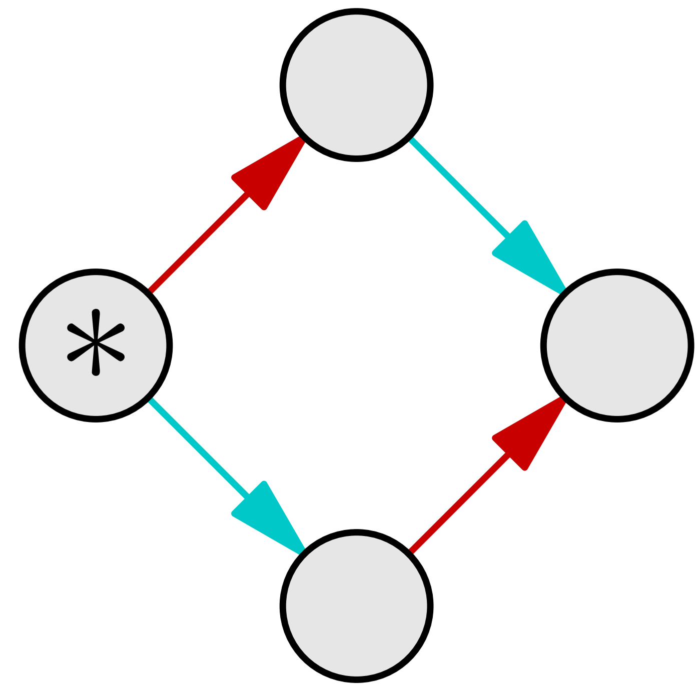
$C_3 \times C_4$



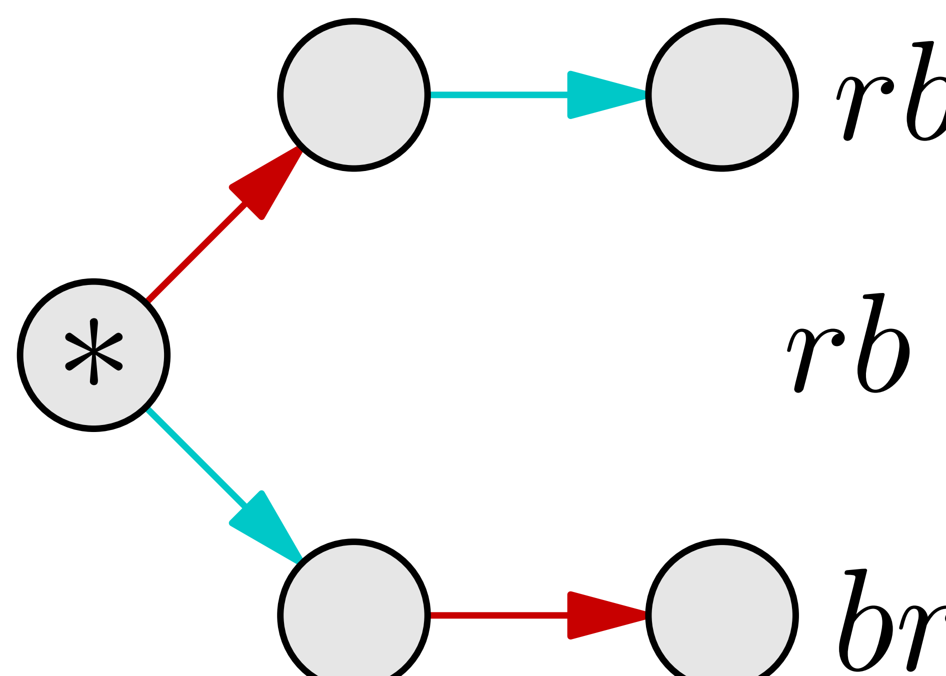
Abelian Groups



$C_3 \times C_4$



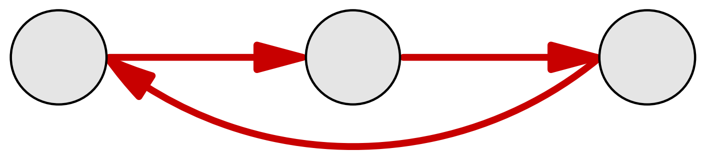
$rb = br$



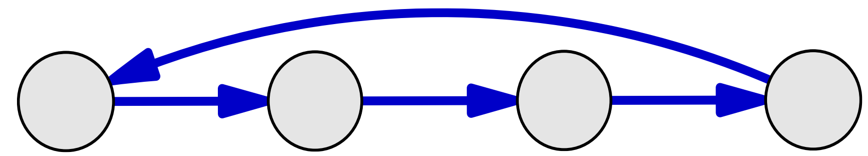
$rb \neq br$

Abelian Groups

1D

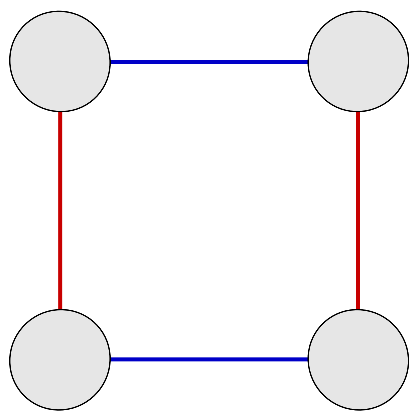


C_3

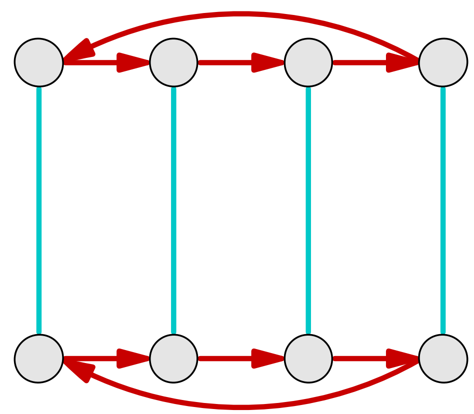


C_4

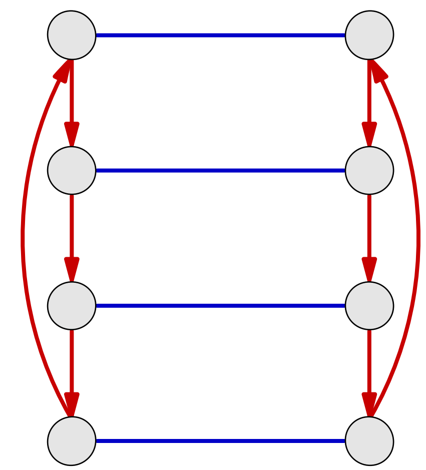
2D



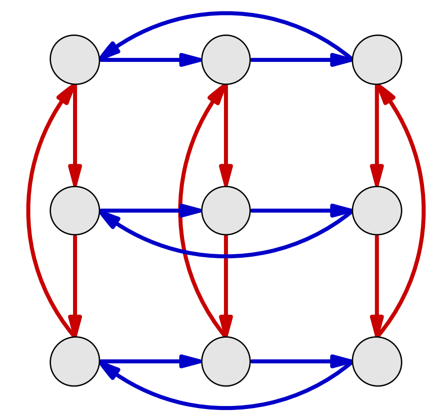
$C_2 \times C_2$



$C_2 \times C_4$

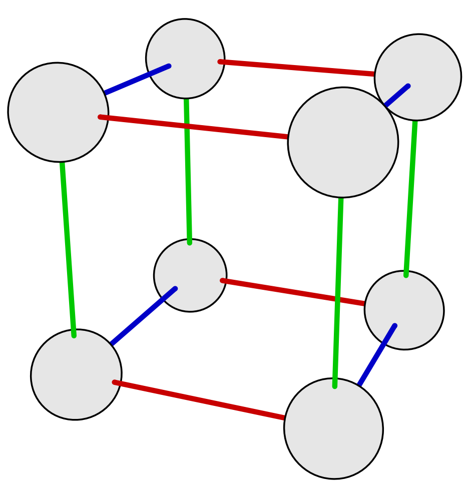


$C_4 \times C_2$

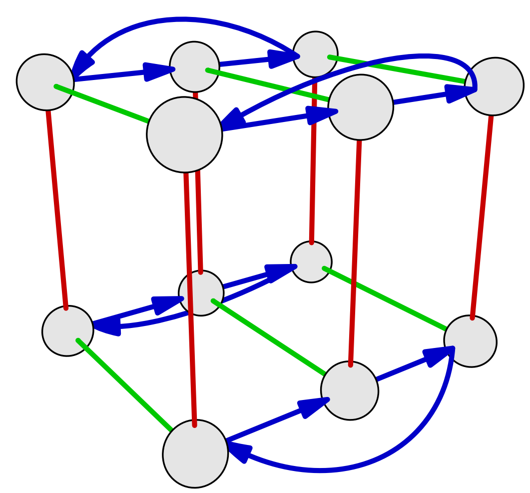


$C_3 \times C_3$

3D



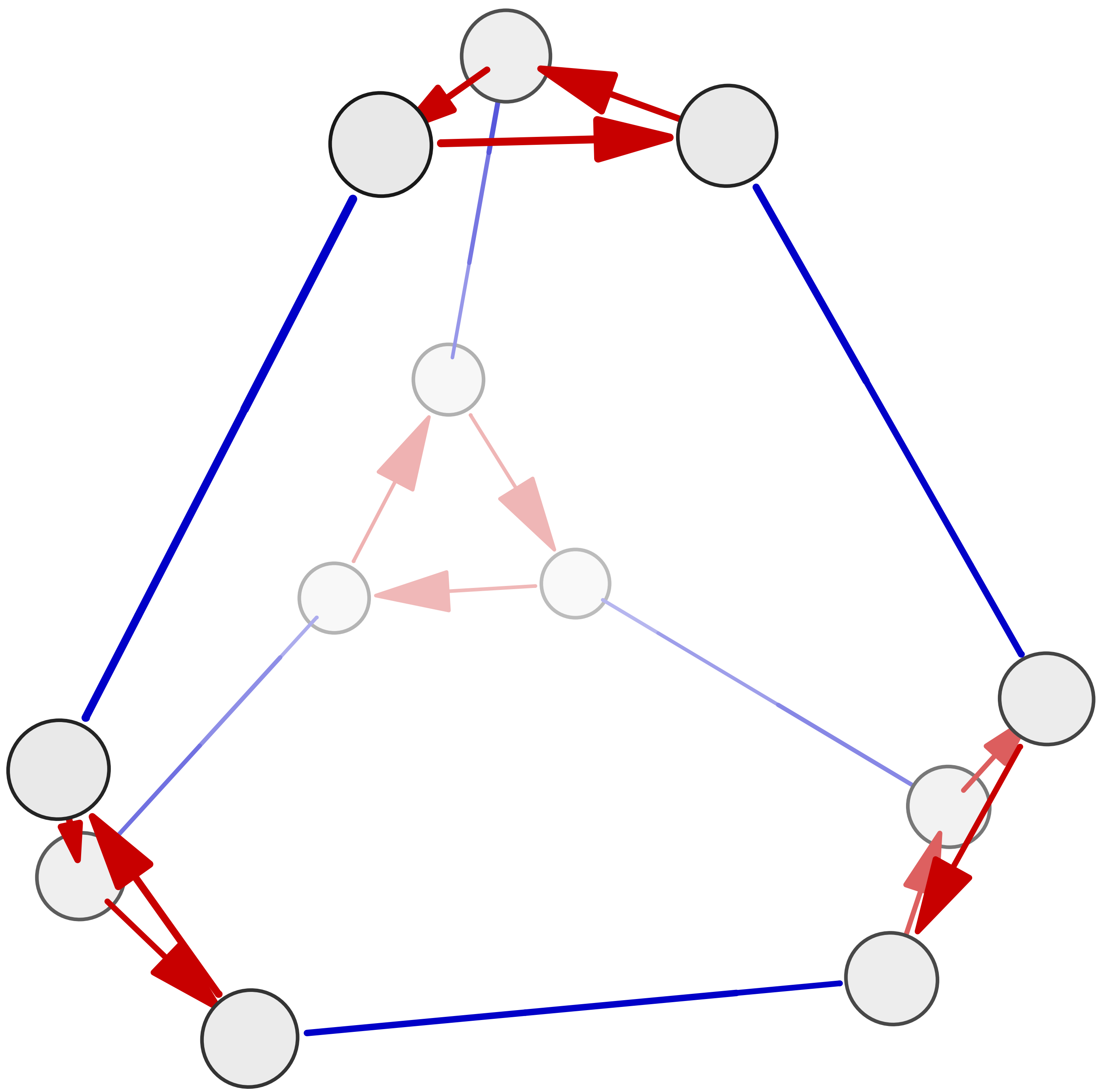
$C_2 \times C_2 \times C_2$



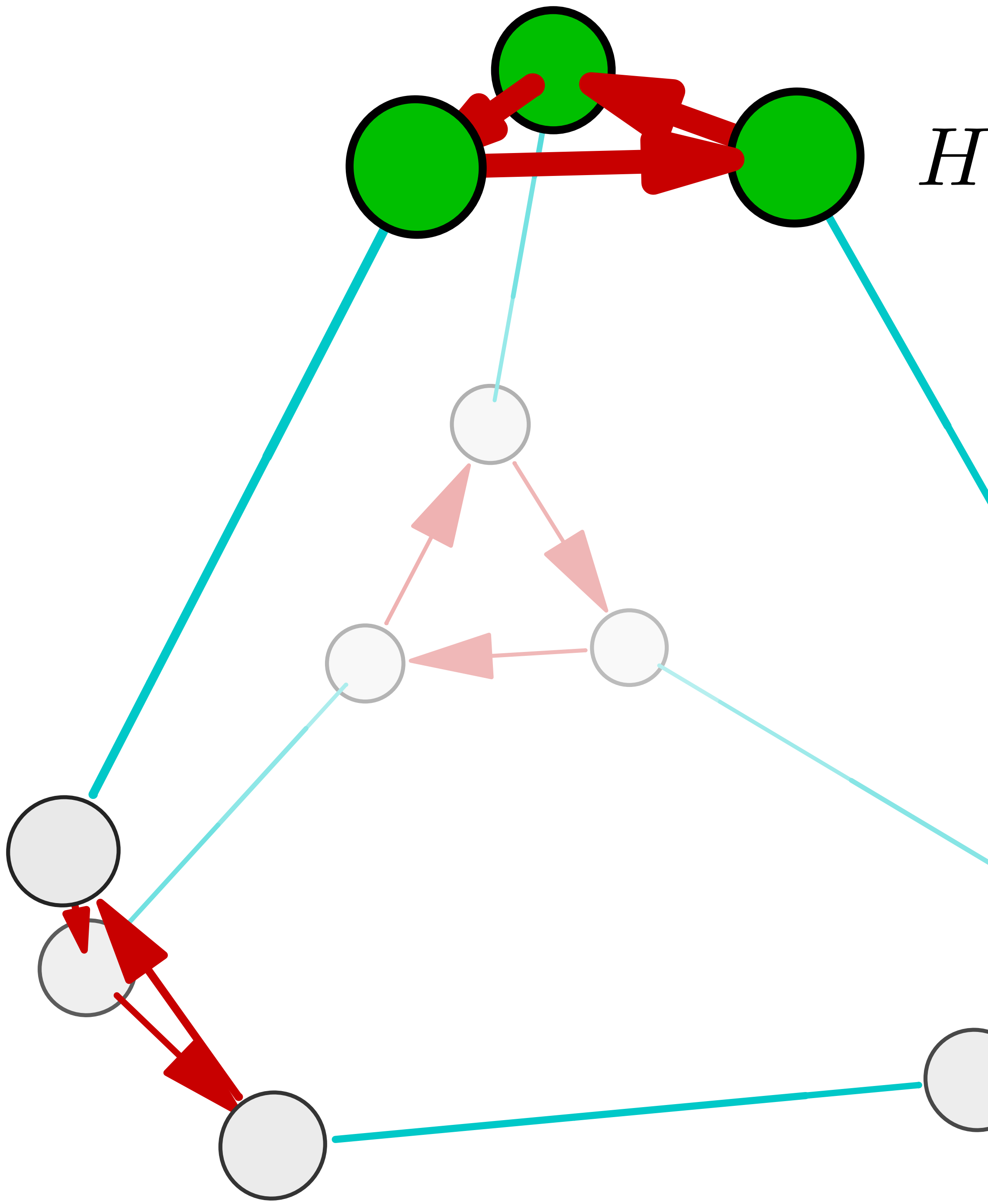
$C_2 \times C_2 \times C_3$

How can we simplify big, complex groups?

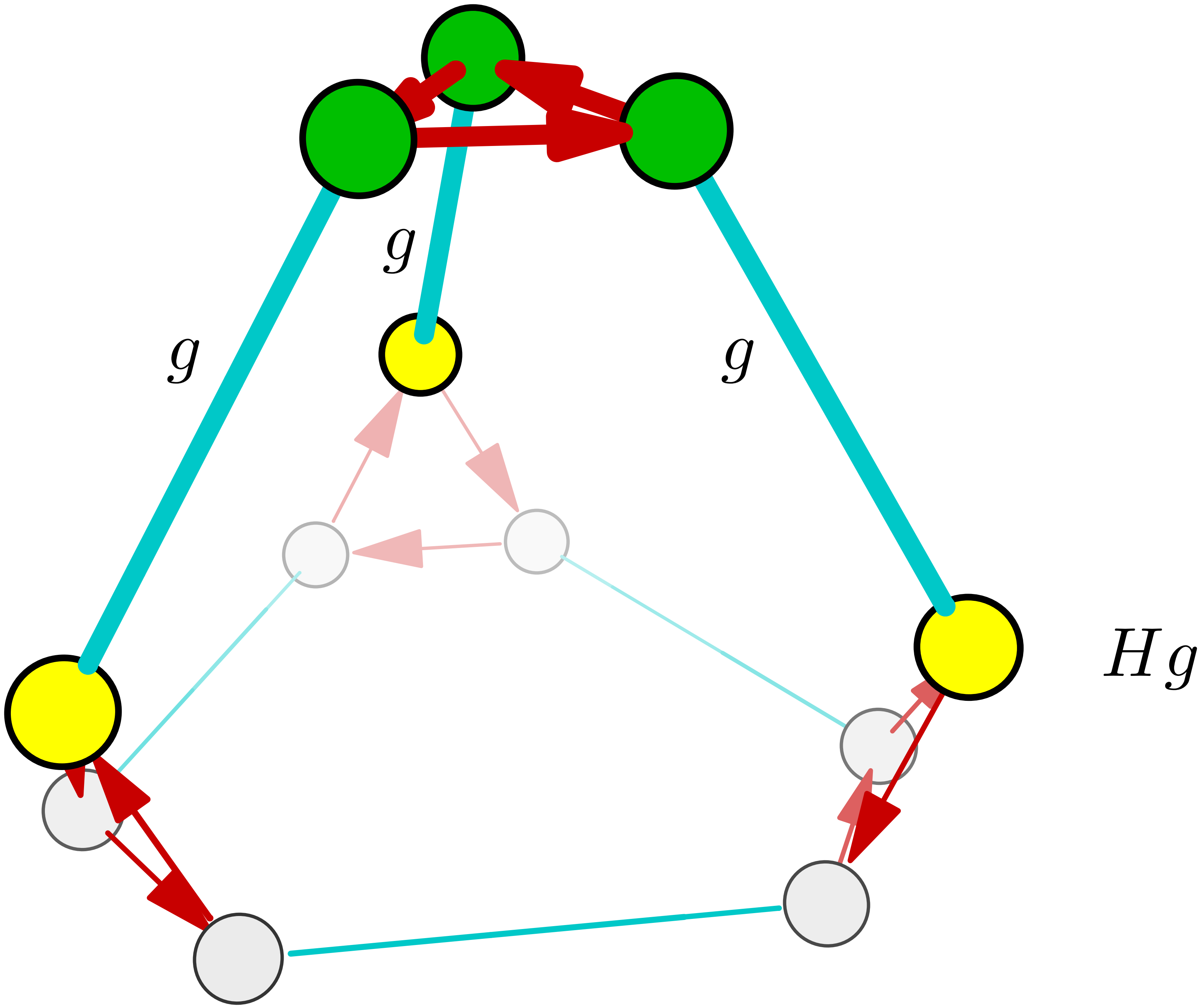
SUBGroups



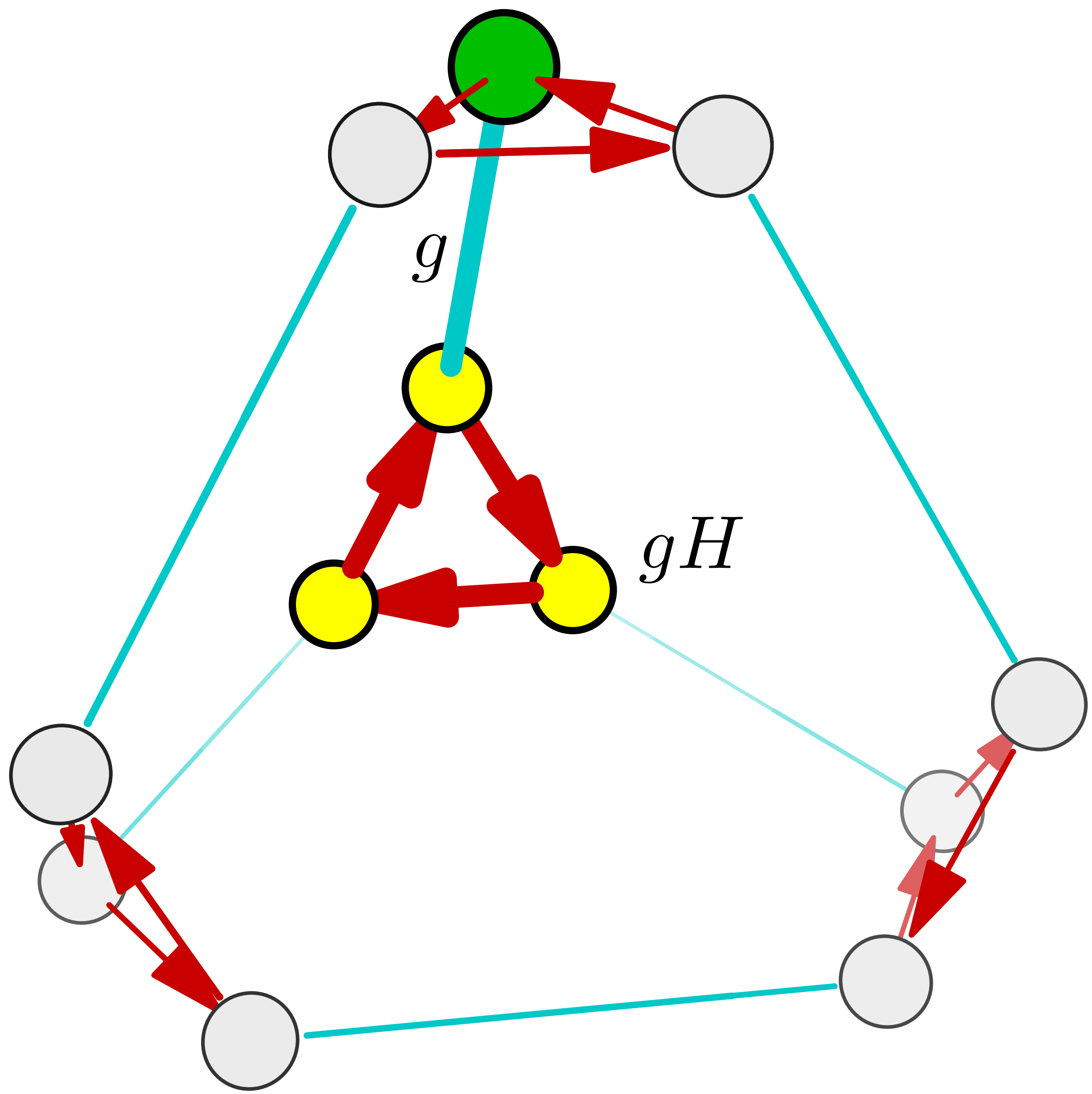
SUBGroups



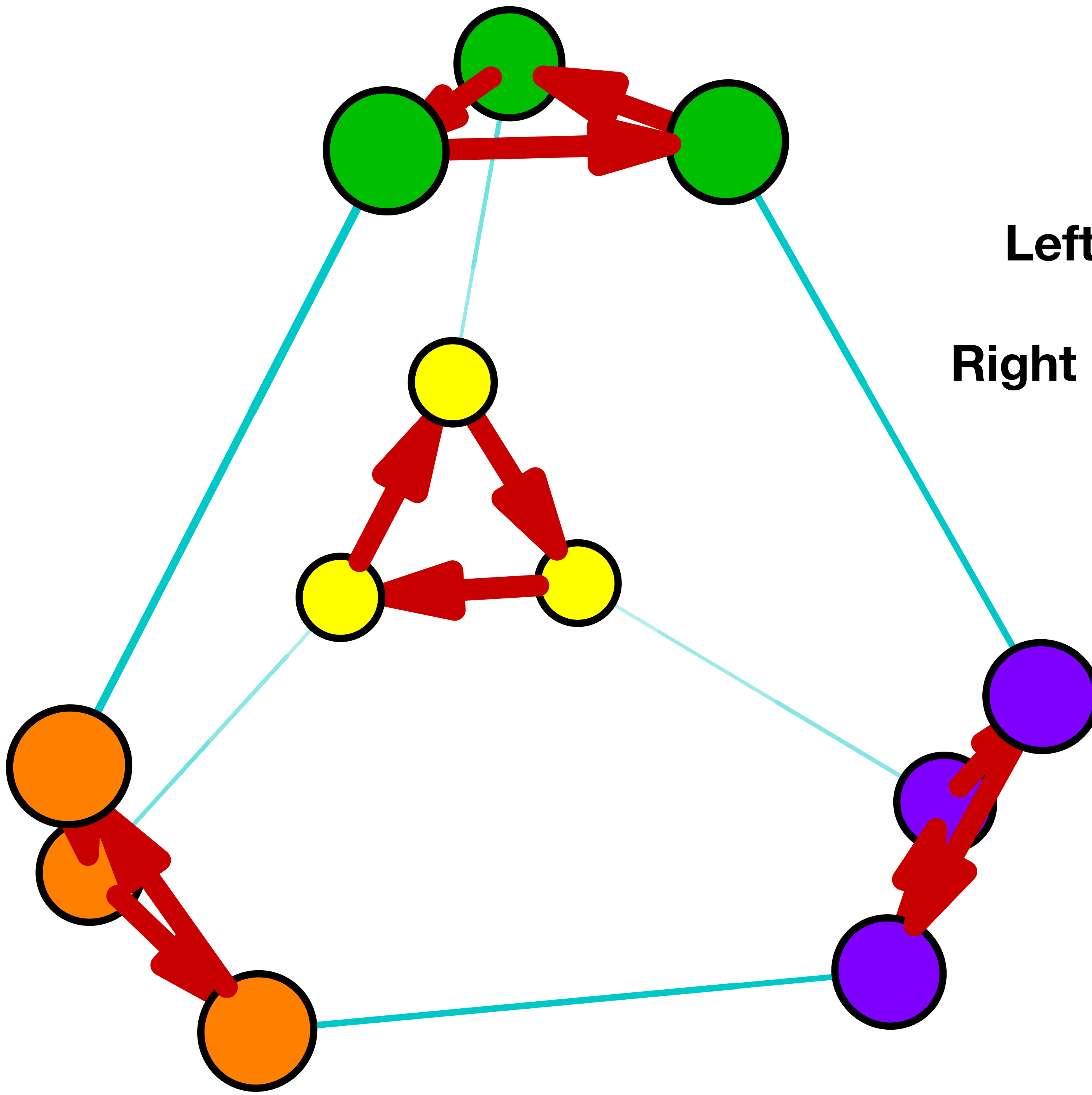
SUBGroups



SUBGroups



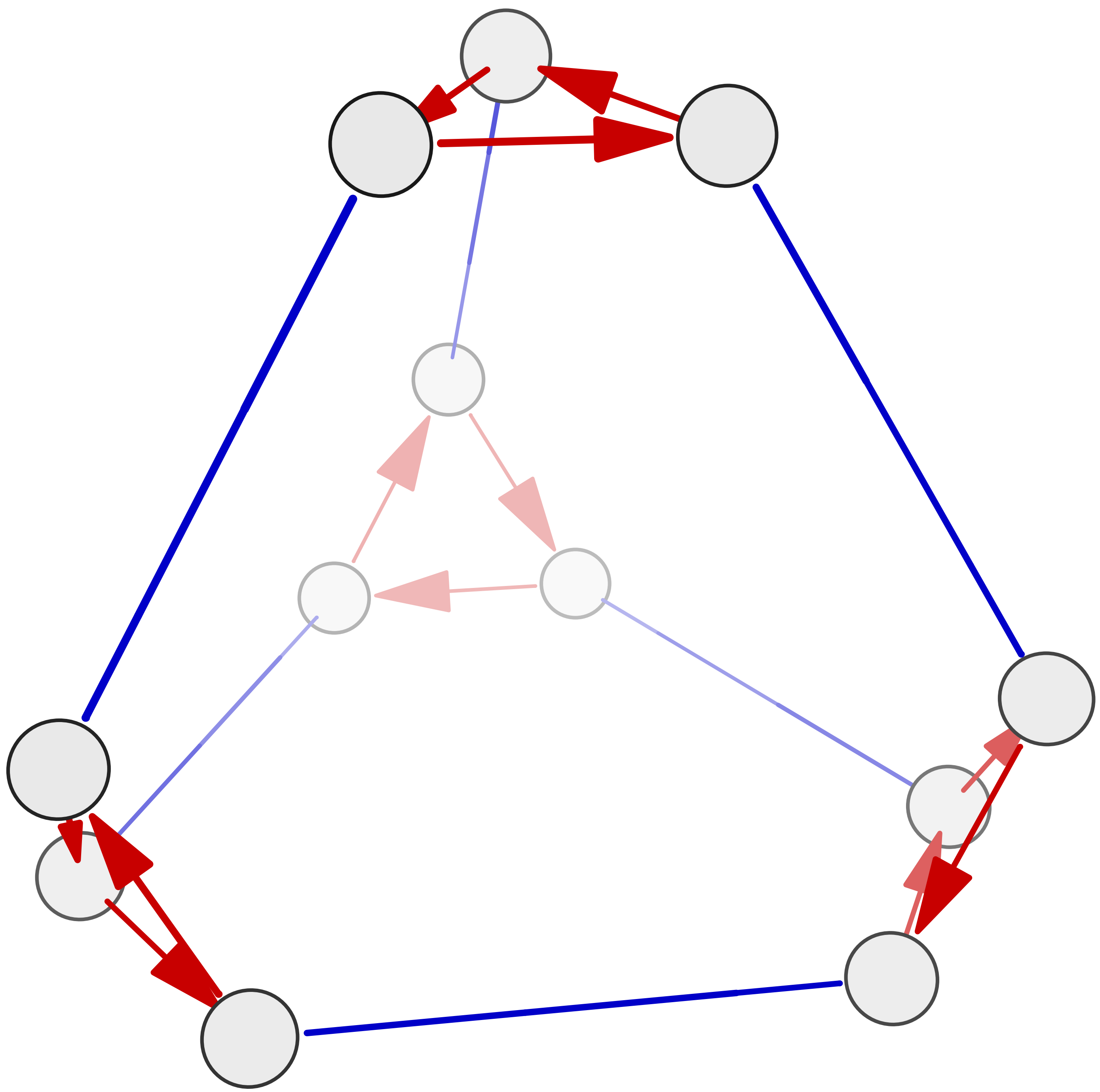
SUBGroups



Left cosets colored

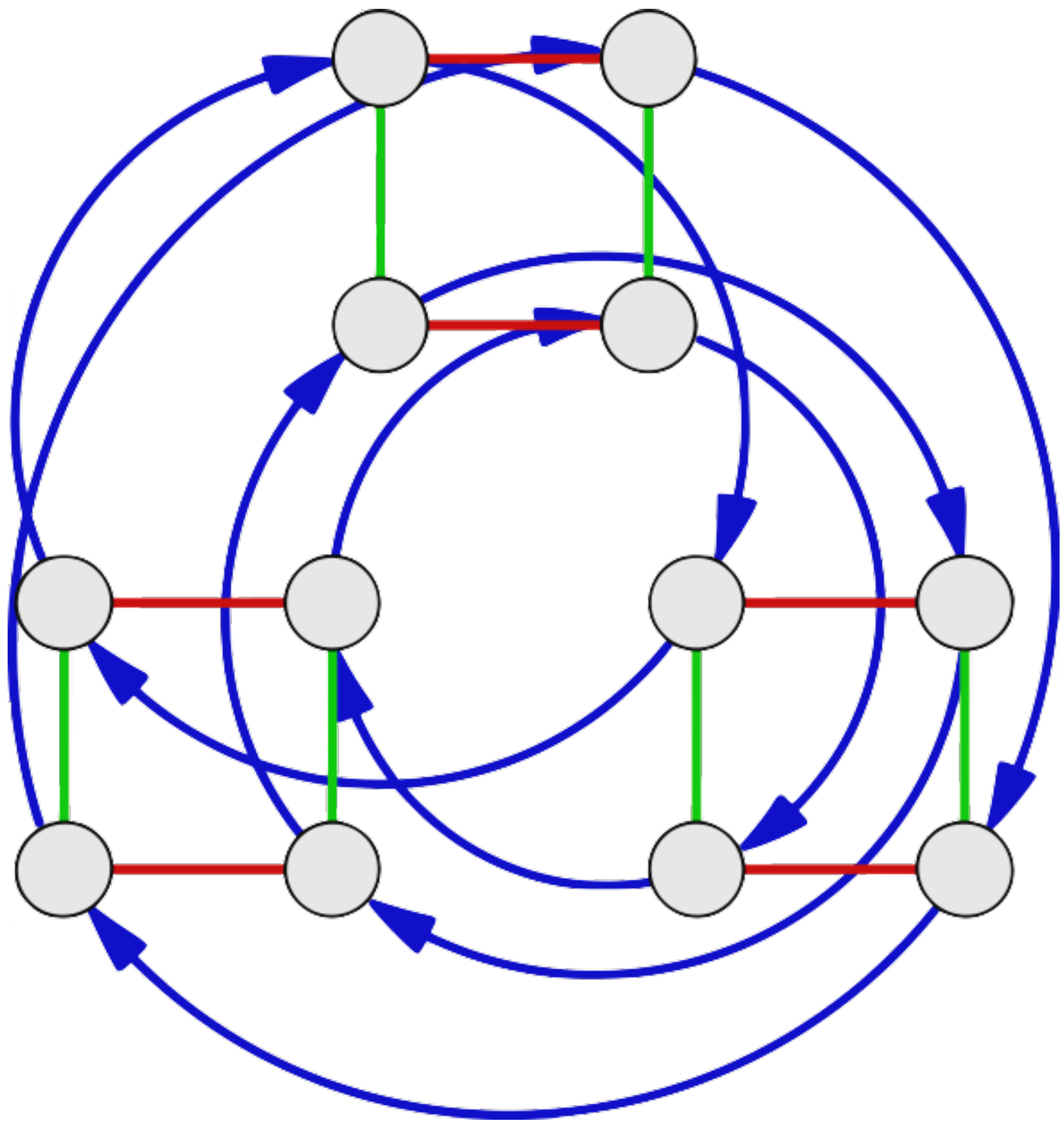
Right cosets are not the same

SUBGroups

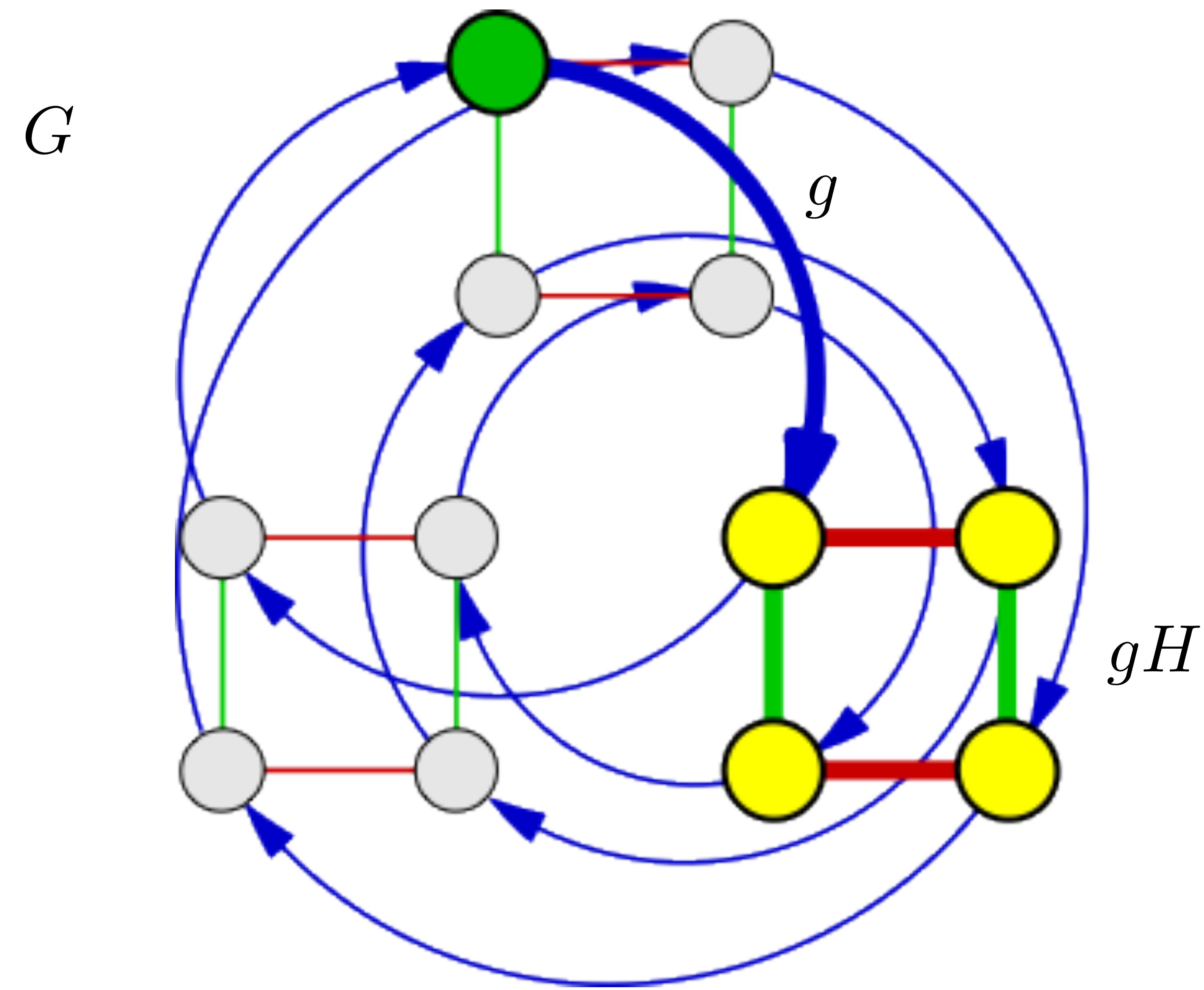


QUOTIENT GROUPS

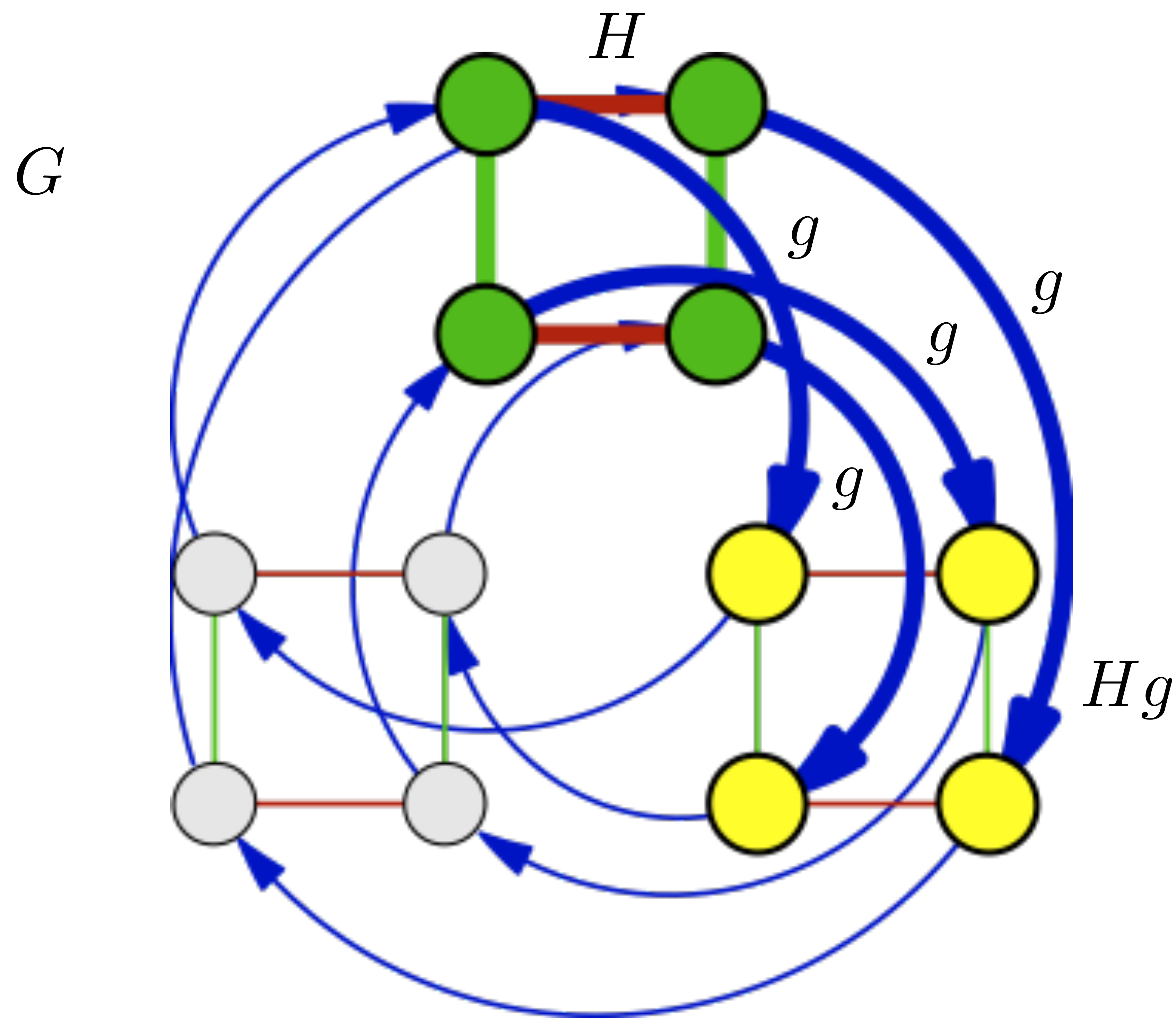
G



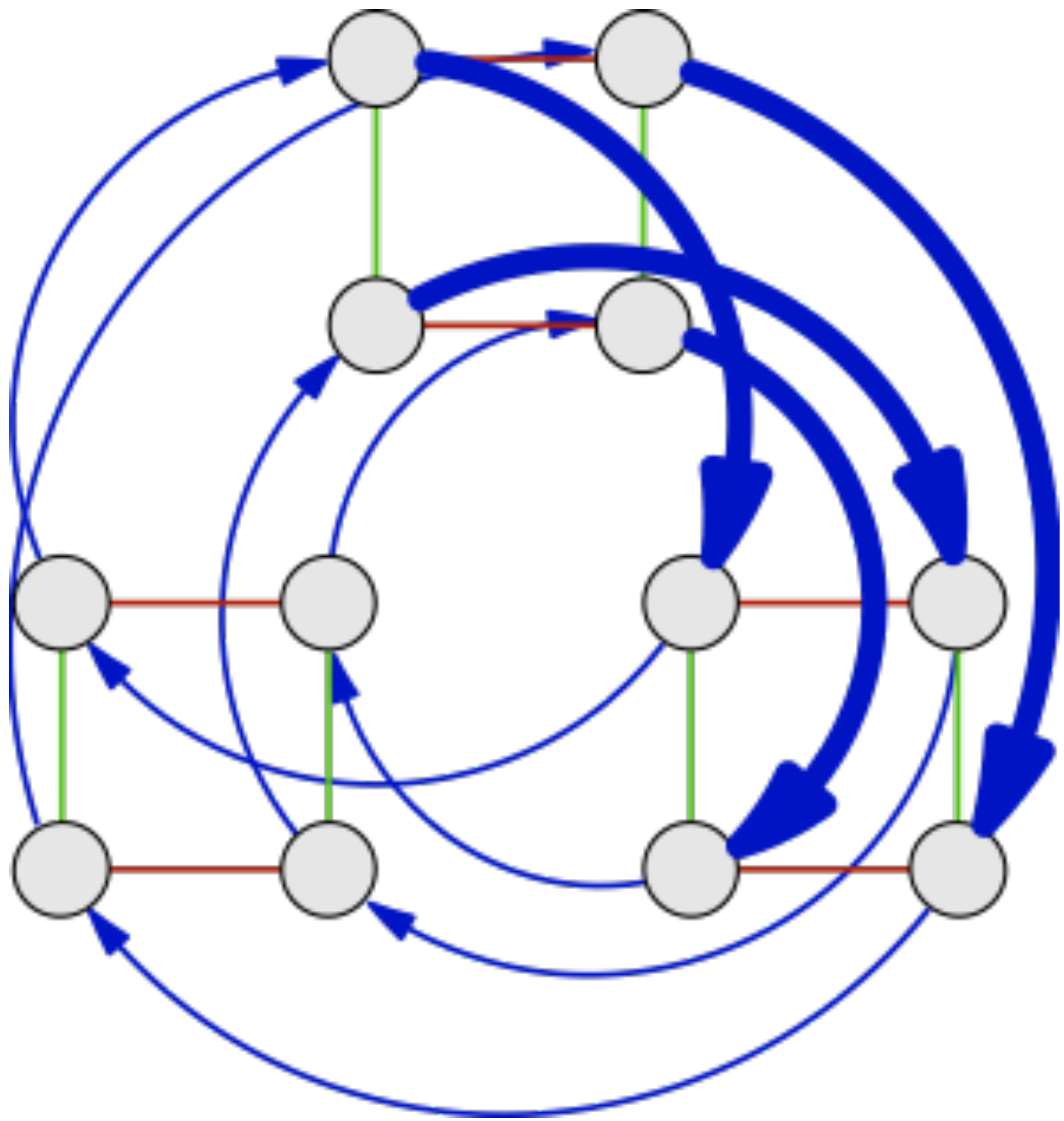
QUOTIENT GROUPS



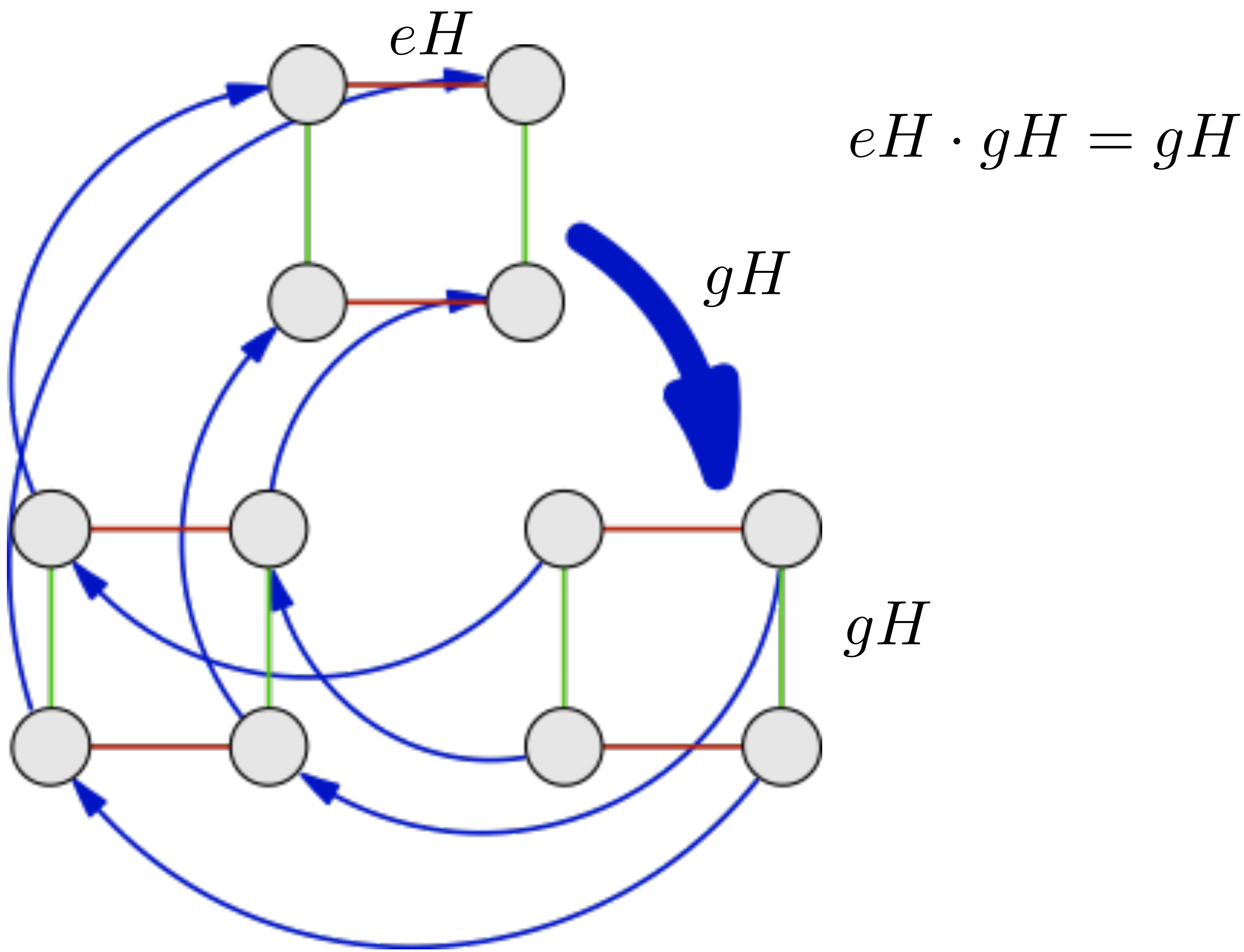
QUOTIENT GROUPS



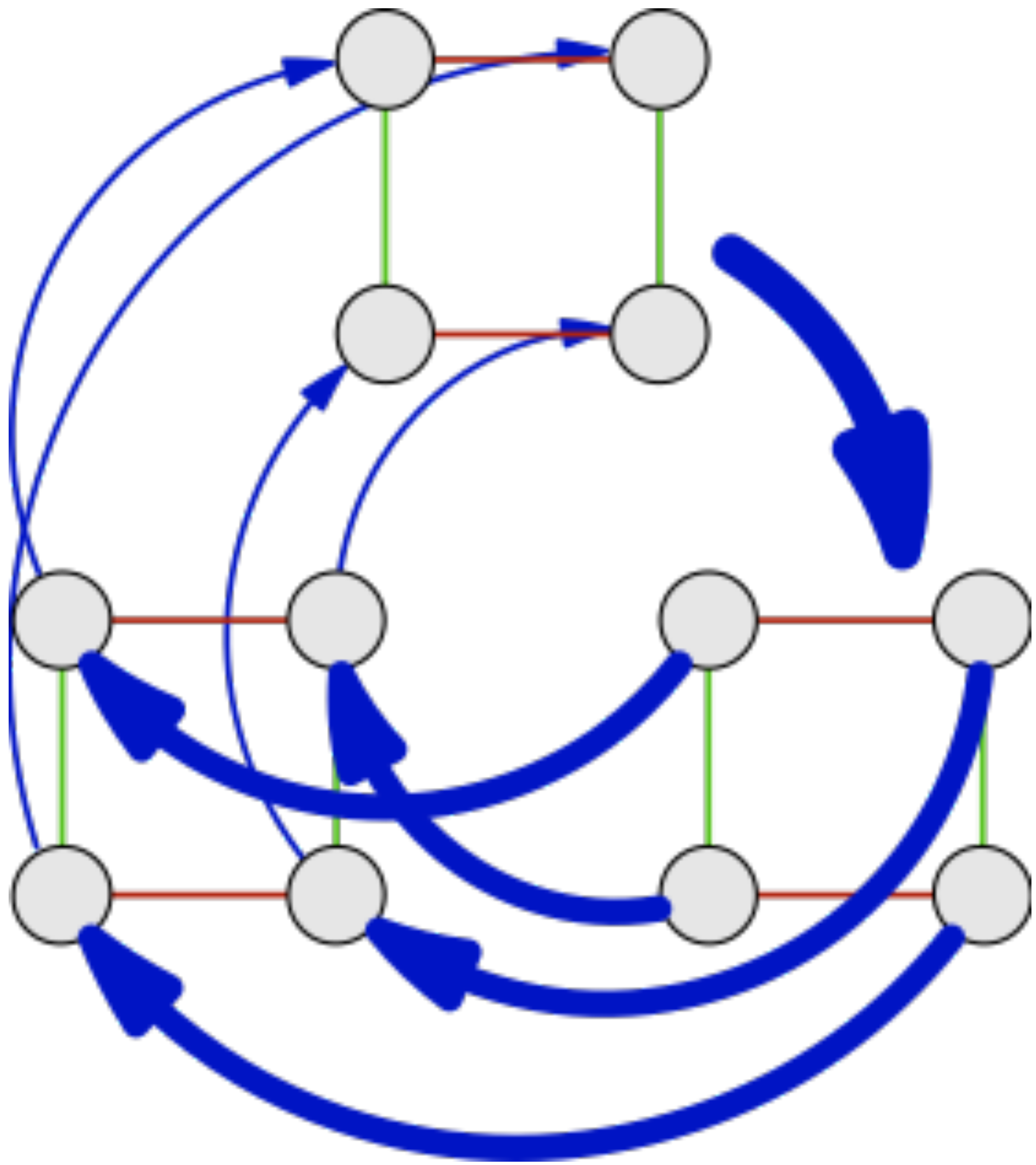
QUOTIENT GROUPS



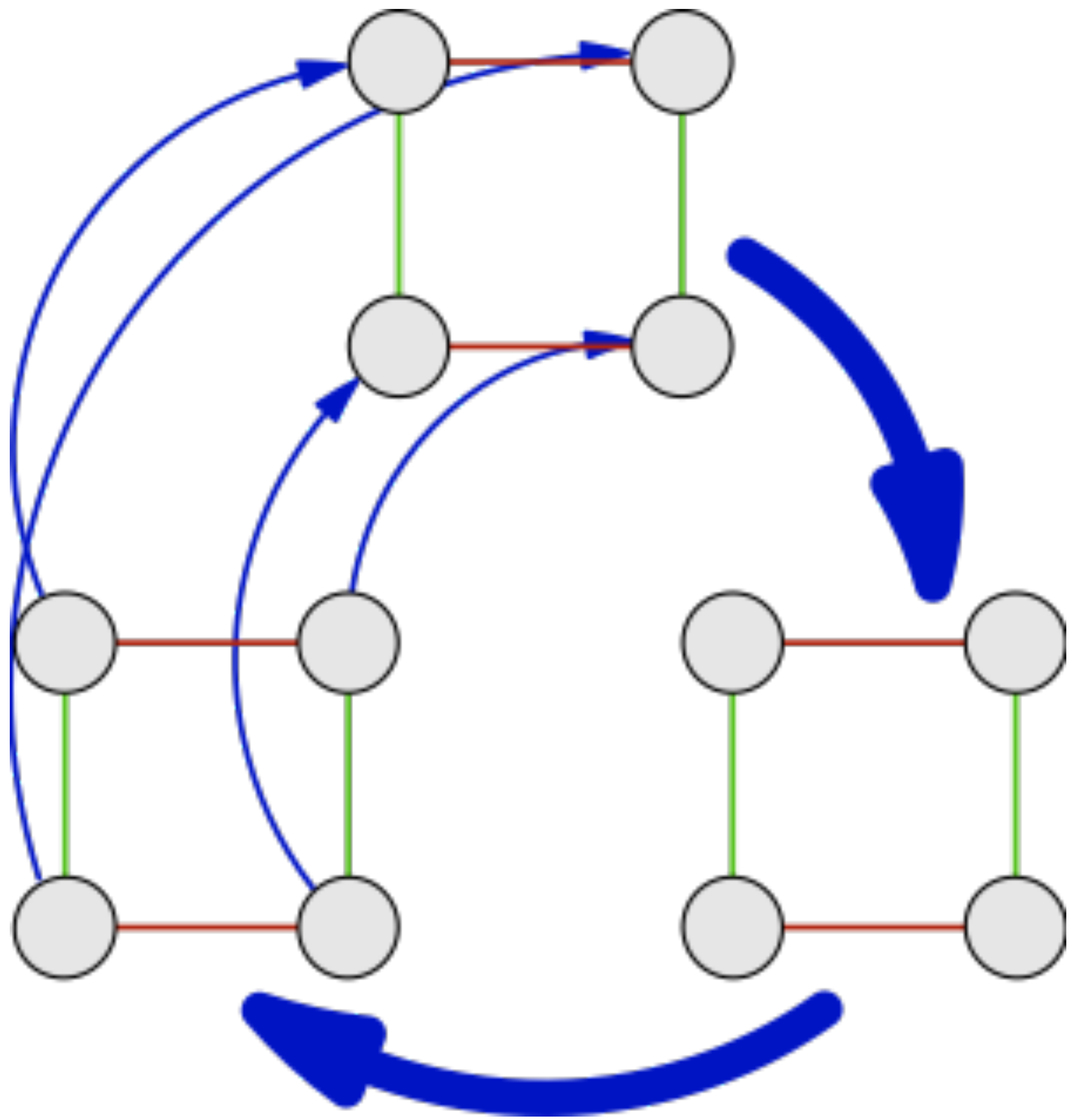
QUOTIENT GROUPS



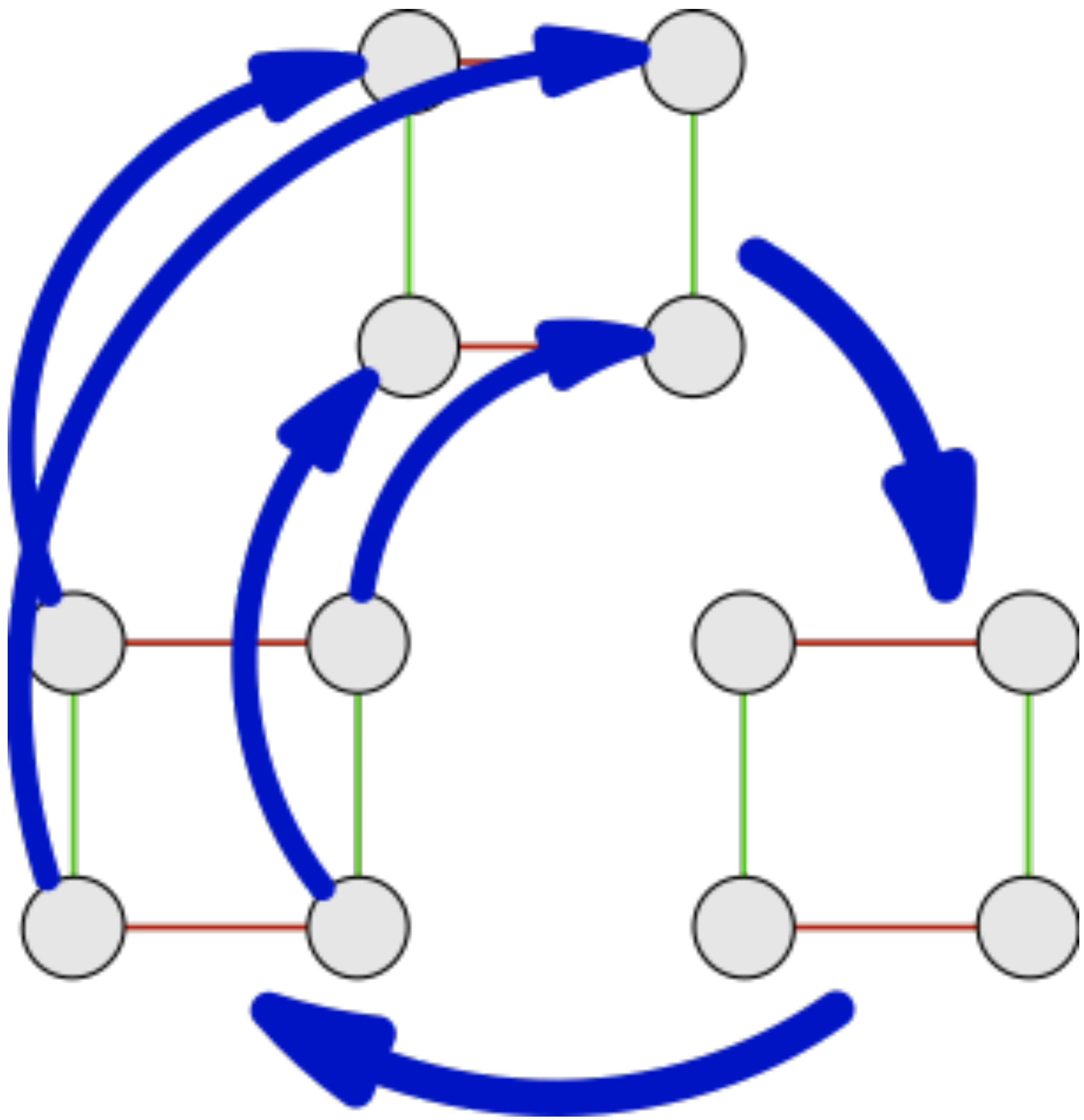
QUOTIENT GROUPS



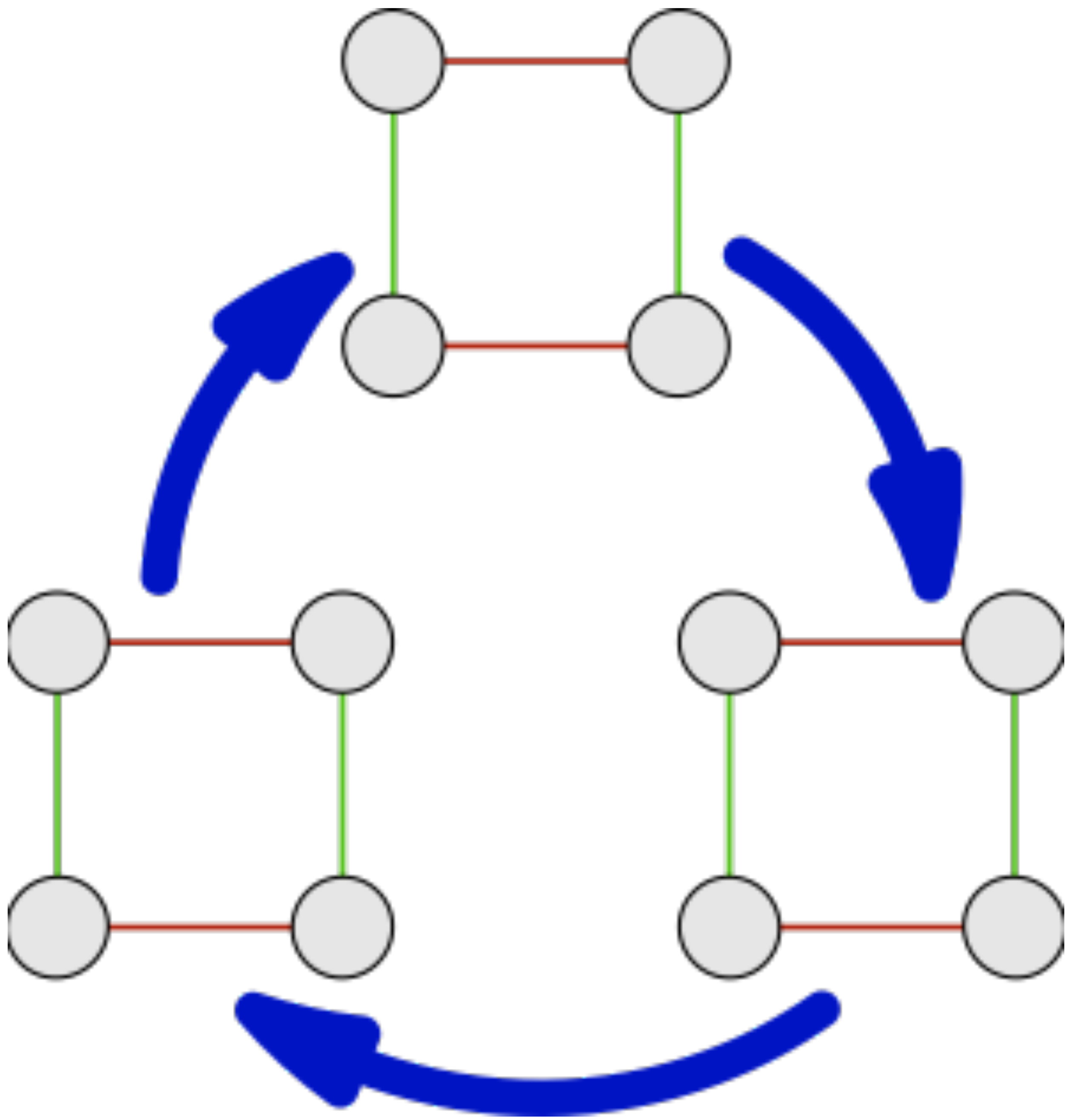
QUOTIENT GROUPS



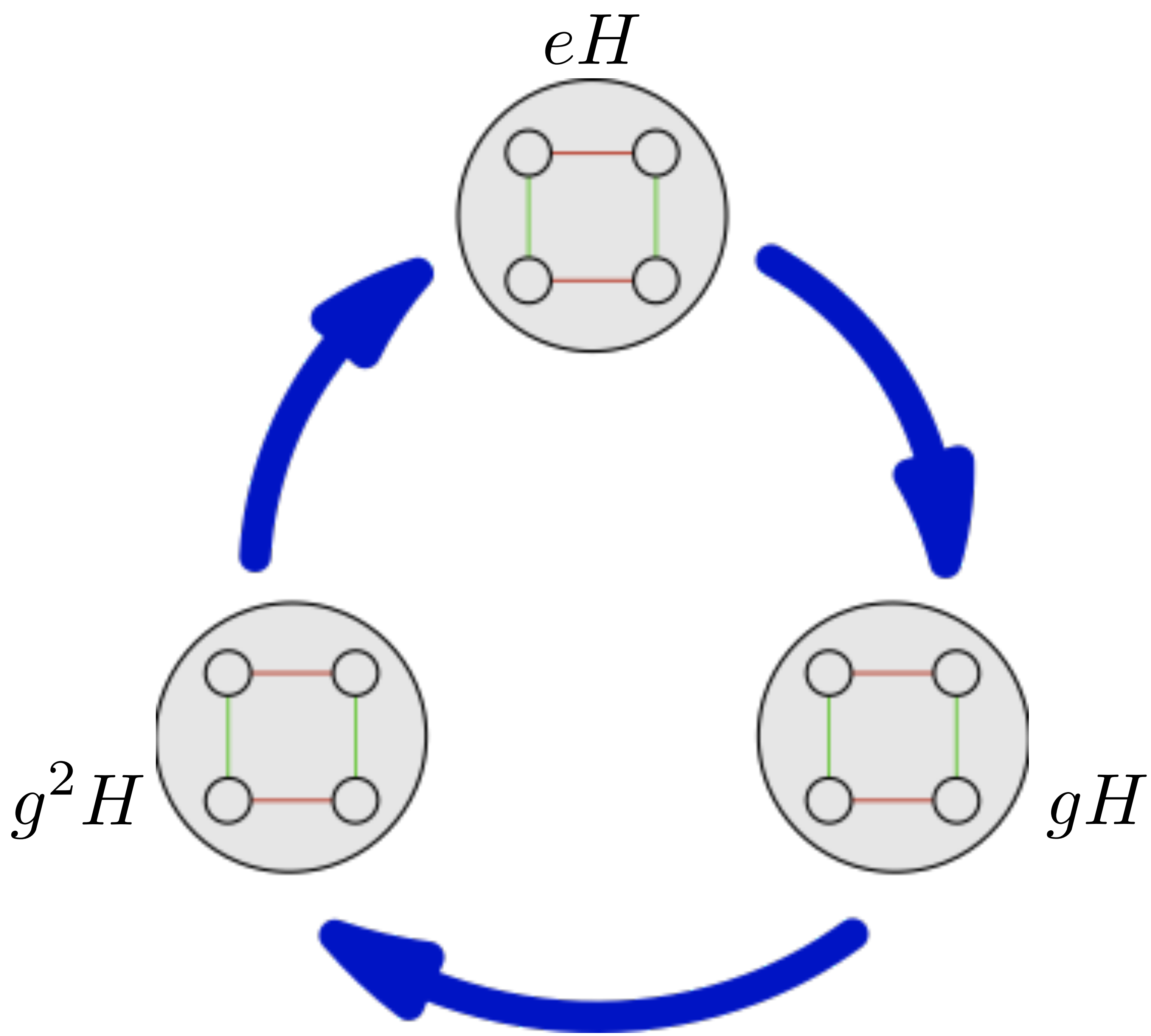
QUOTIENT GROUPS



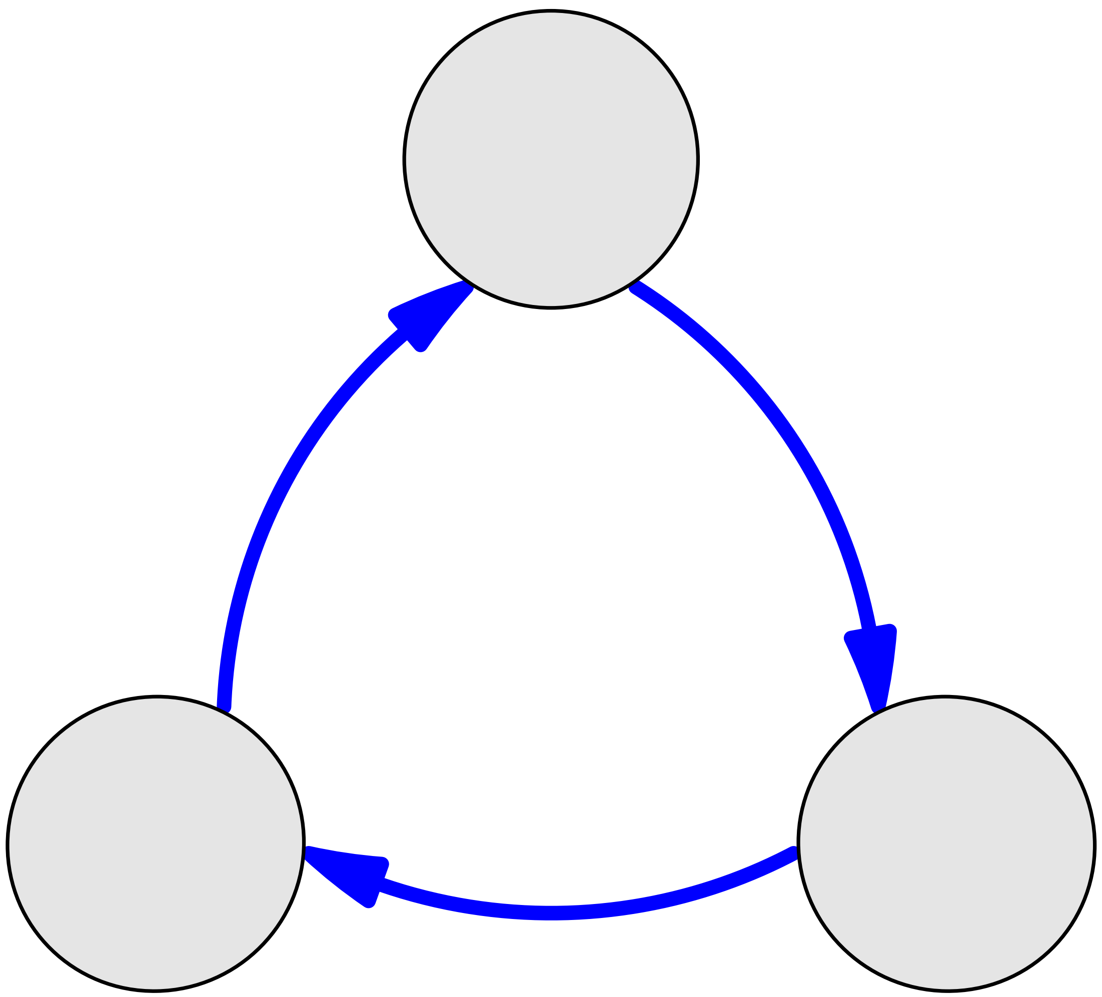
QUOTIENT GROUPS



QUOTIENT GROUPS



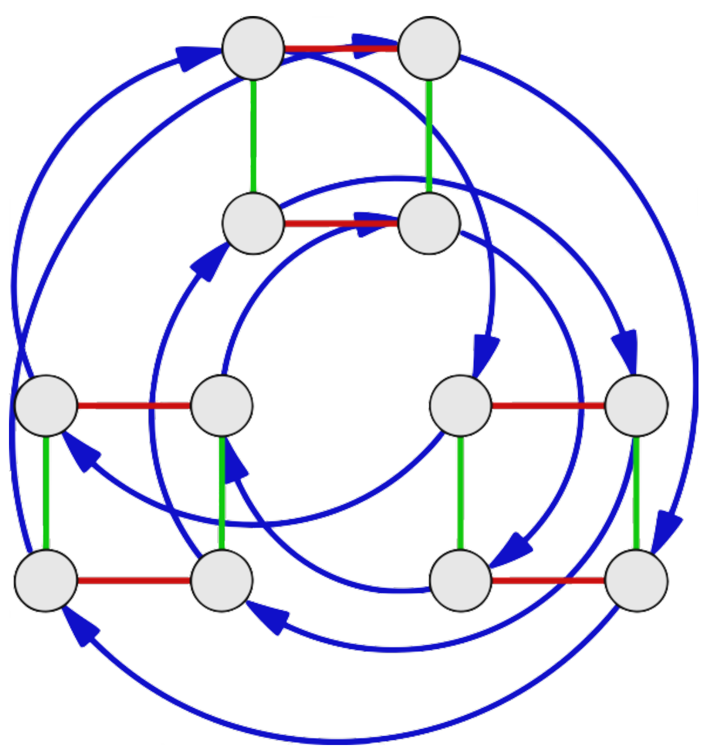
QUOTIENT GROUPS



C_3

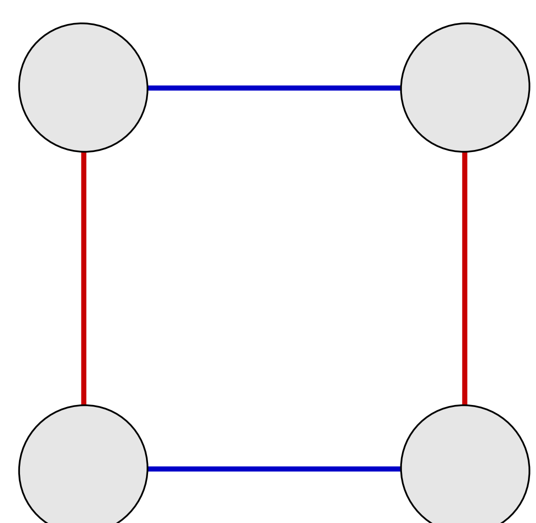
Group Quotients

$$\frac{A_4}{V_4} \cong C_3$$



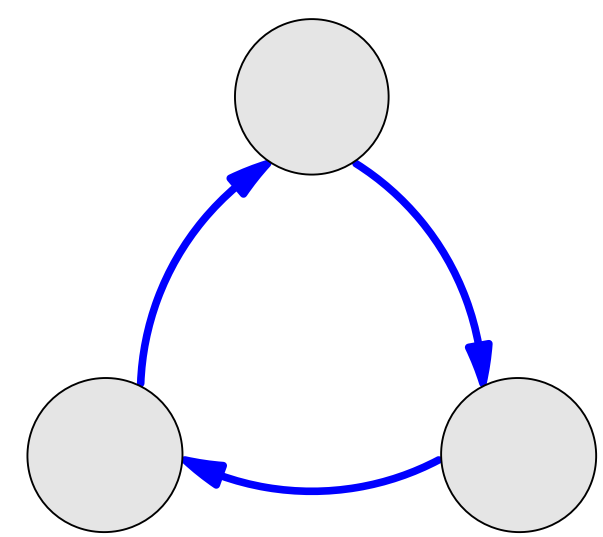
A_4

$/$



V_4

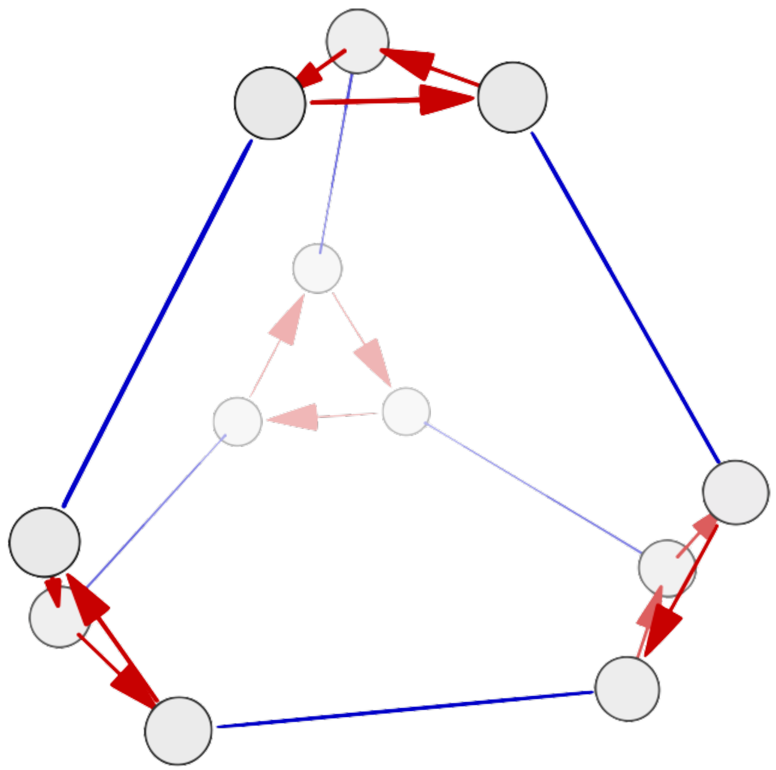
$\cong$



C_3

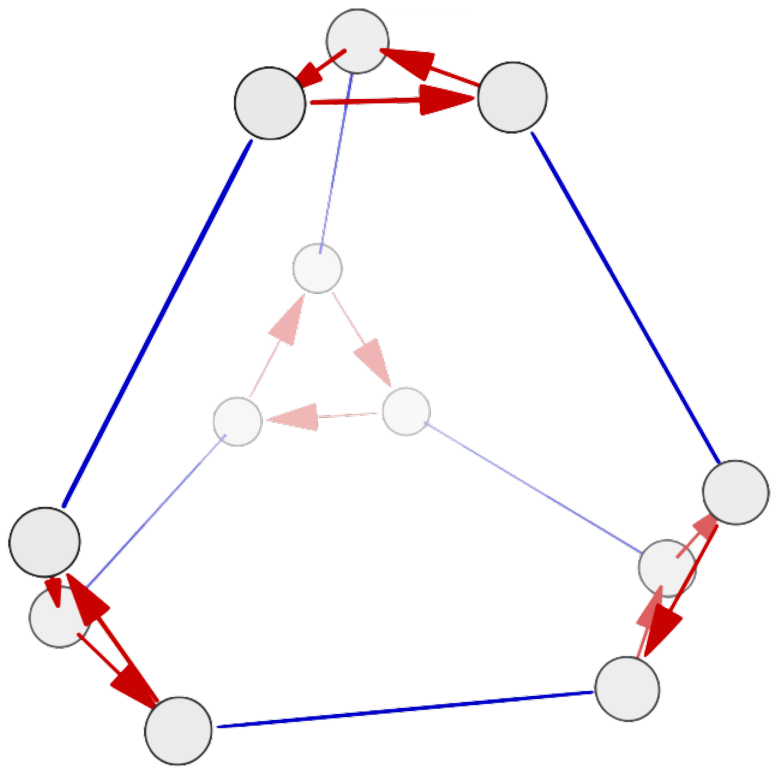
Not All “Quotients” Succeed

Not All “Quotients” Succeed

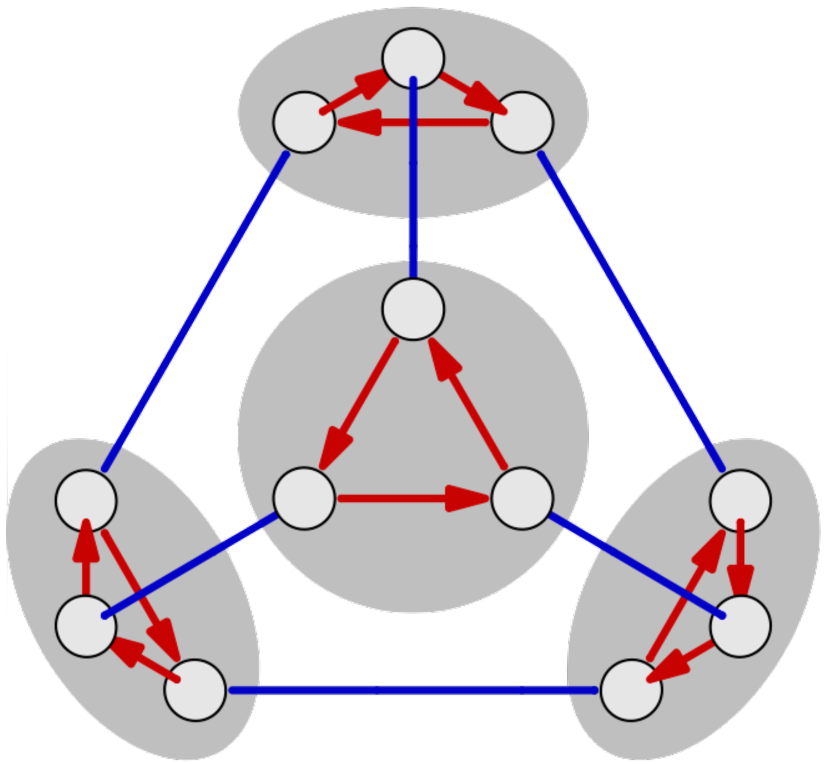


A_4

Not All “Quotients” Succeed

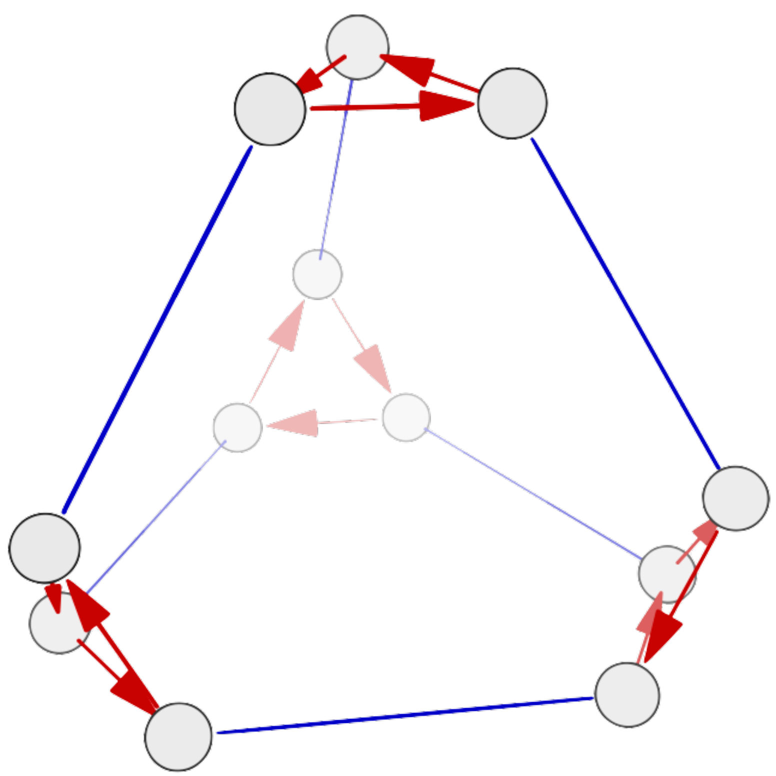


$$A_4$$

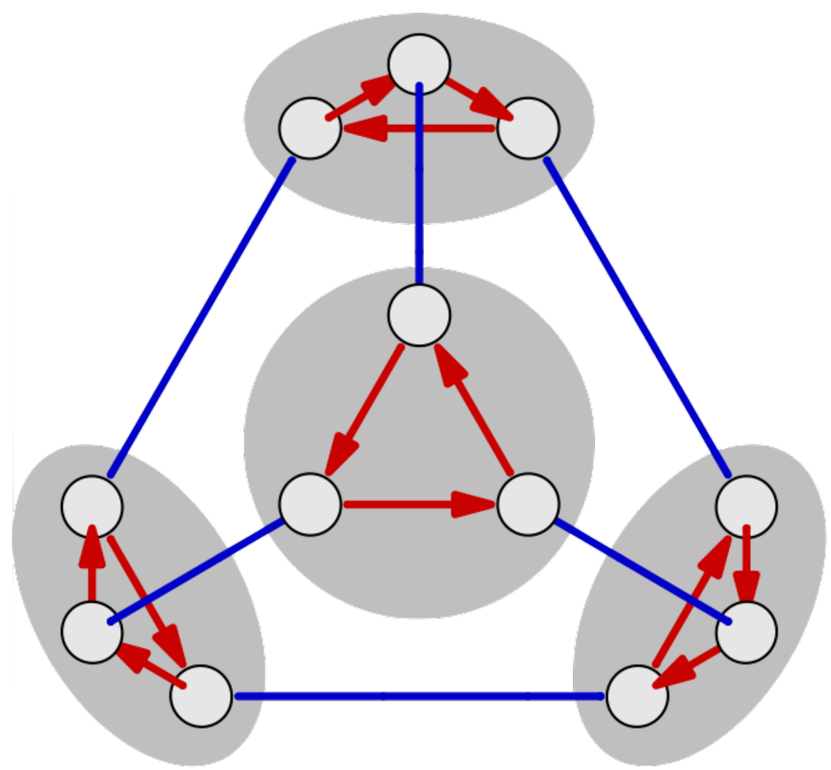


$$\frac{A_4}{C_3}?$$

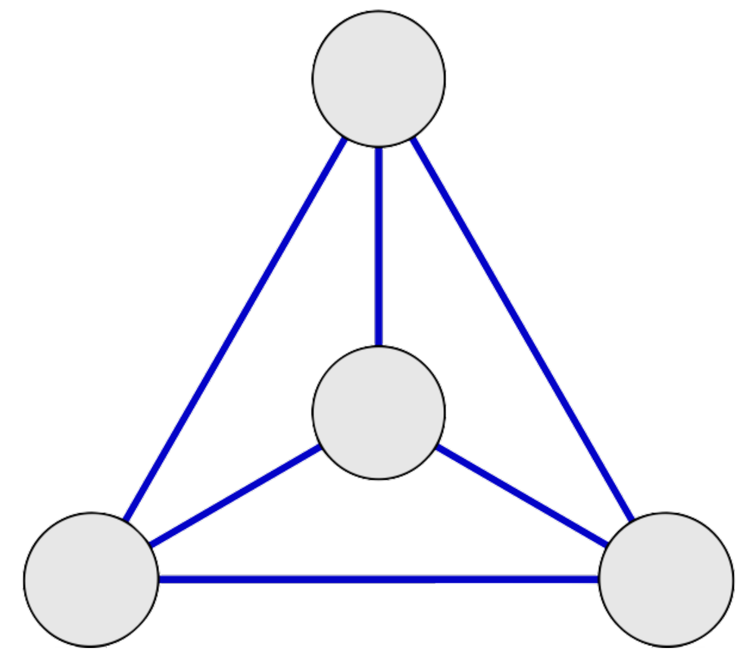
Not All “Quotients” Succeed



A_4



$\frac{A_4}{C_3}$?

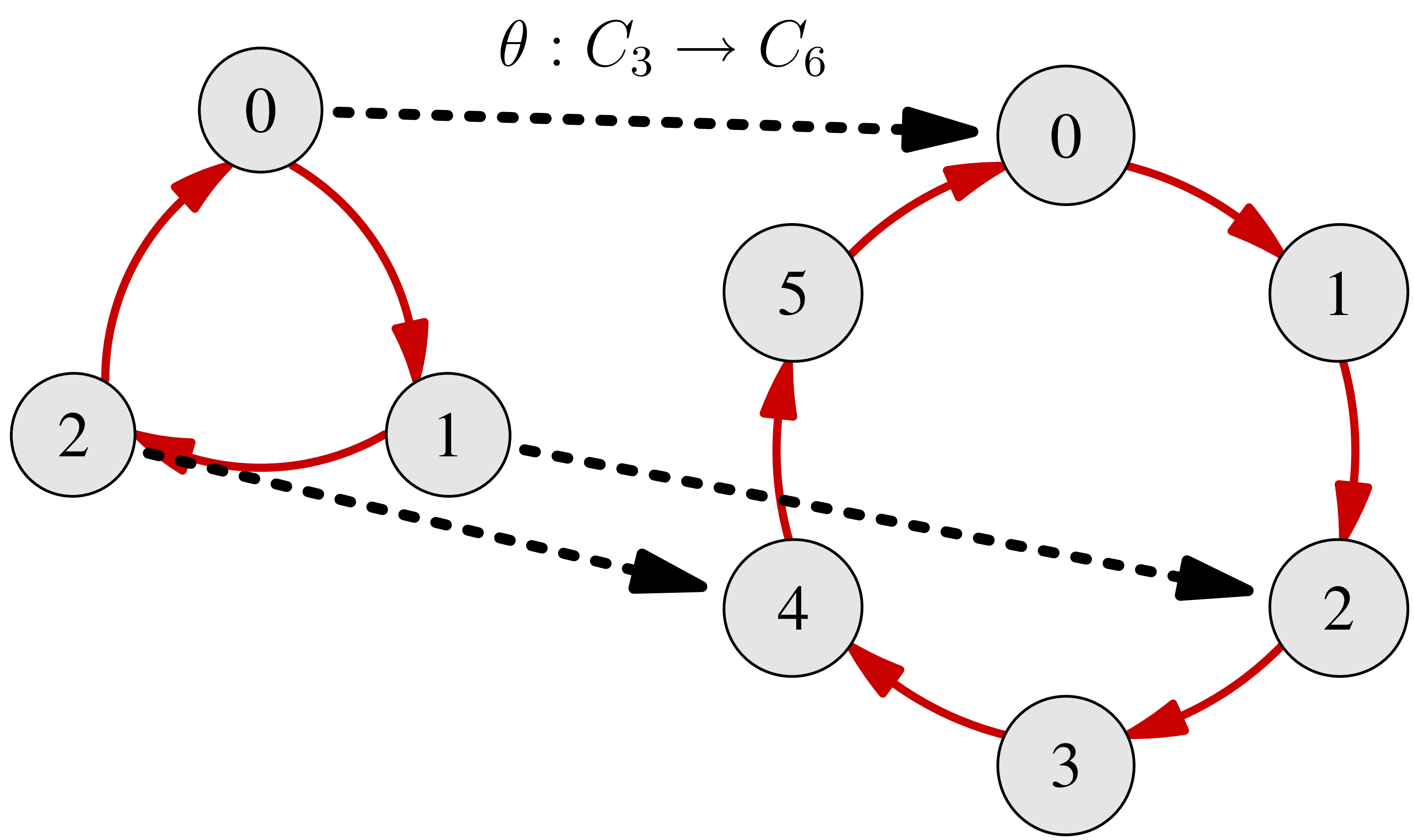


???

Can we compare groups?

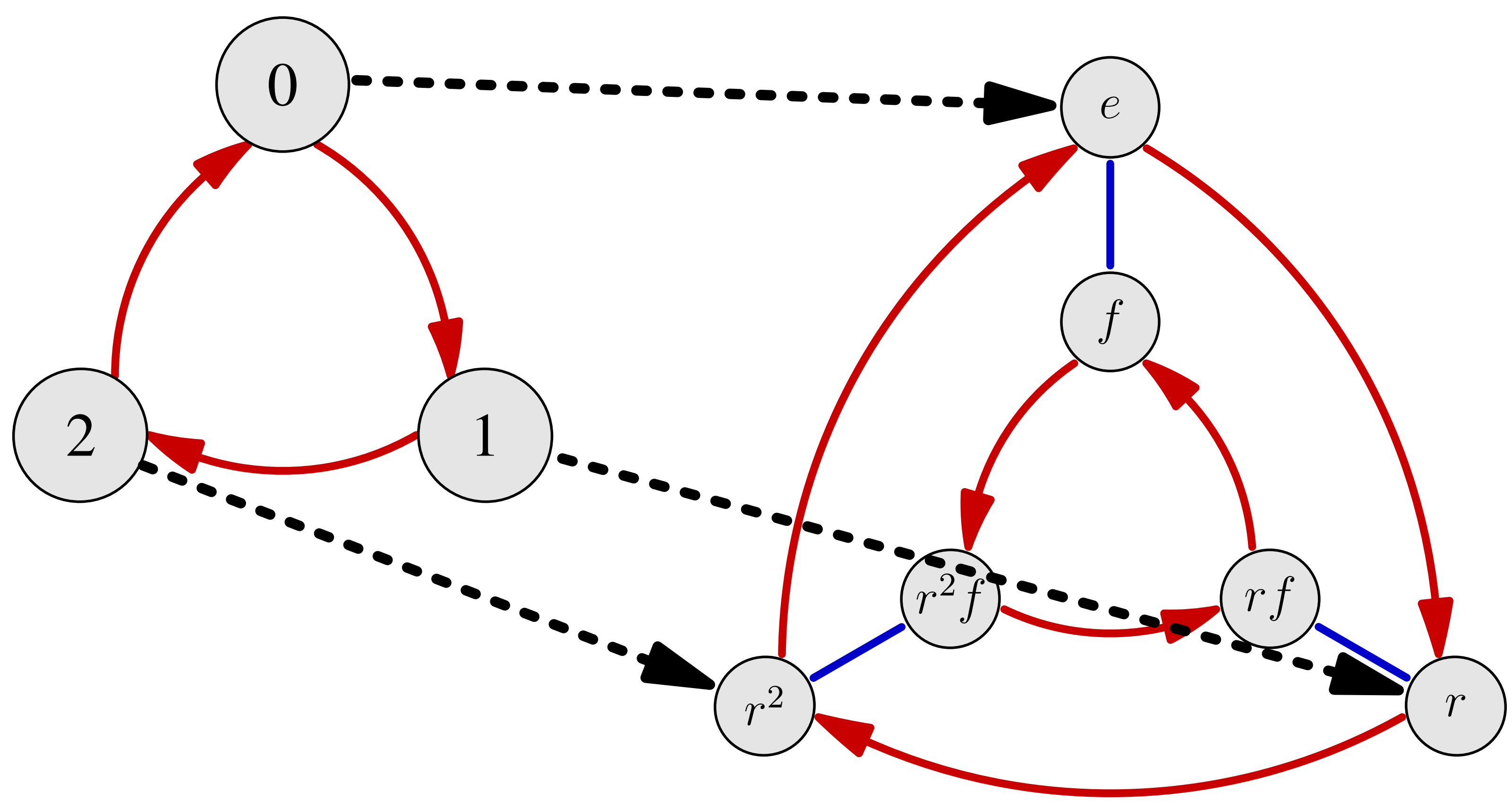
Homomorphisms

Example embedding



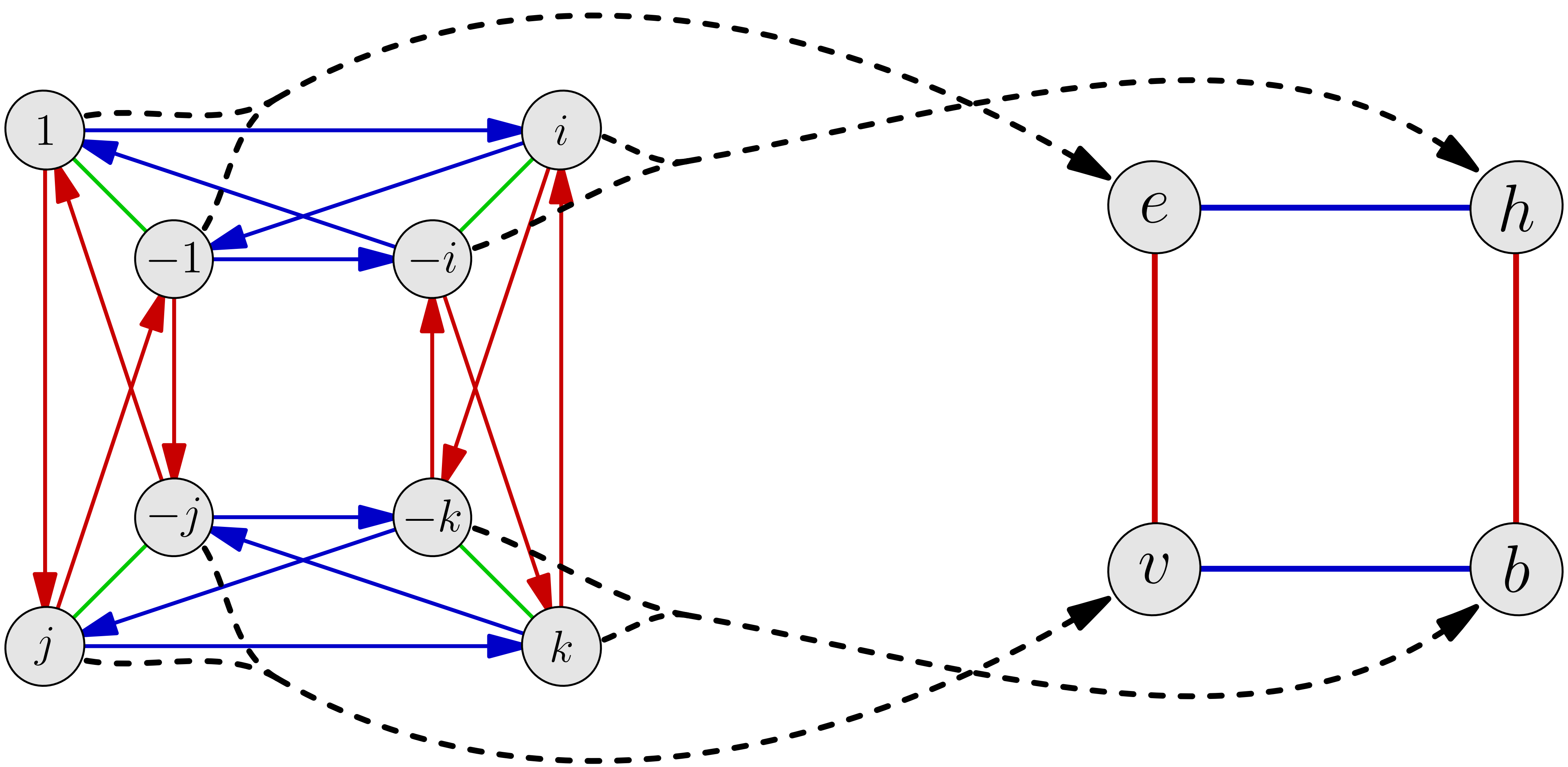
Homomorphisms

Example embedding



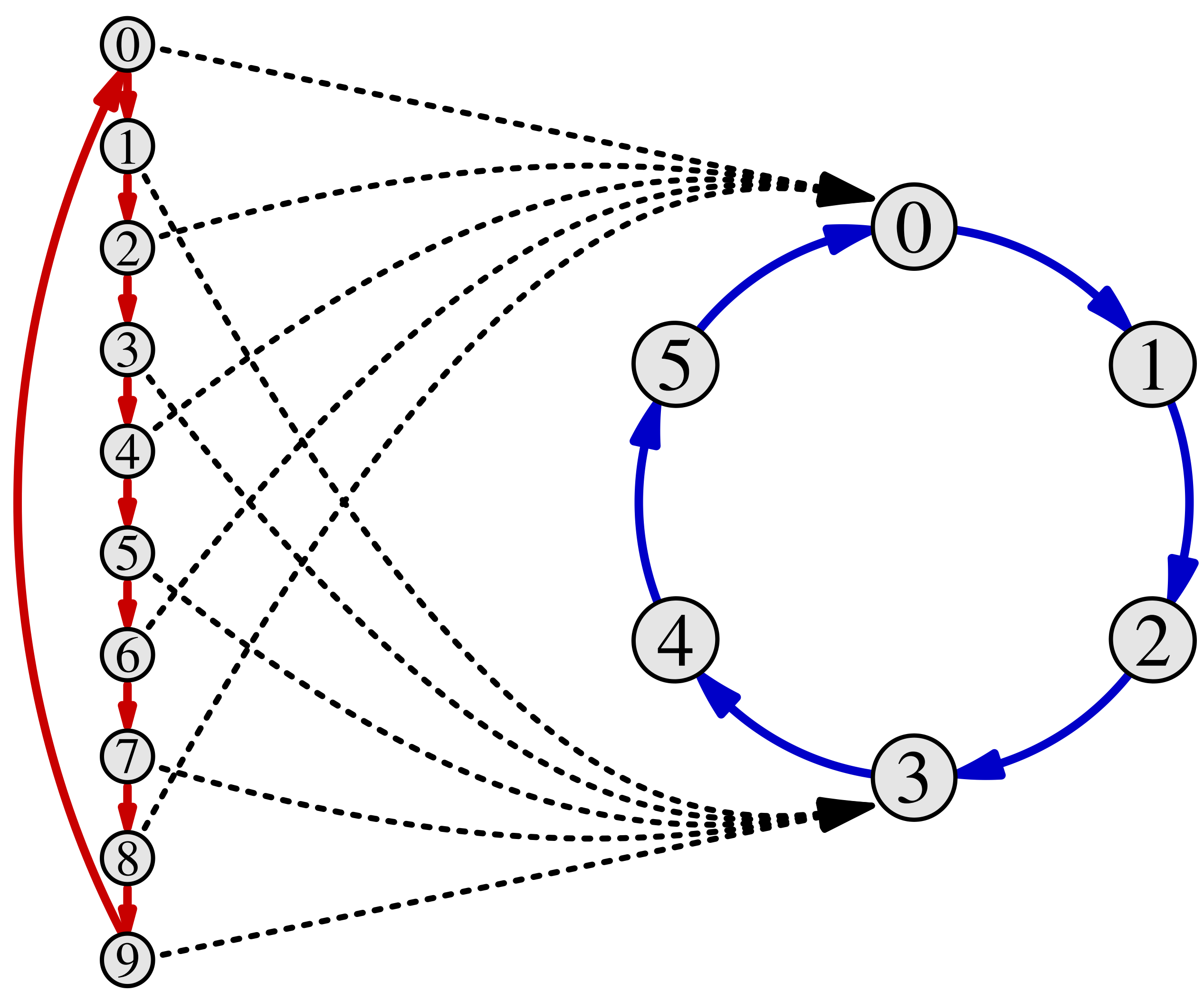
Homomorphisms

Example non-embedding

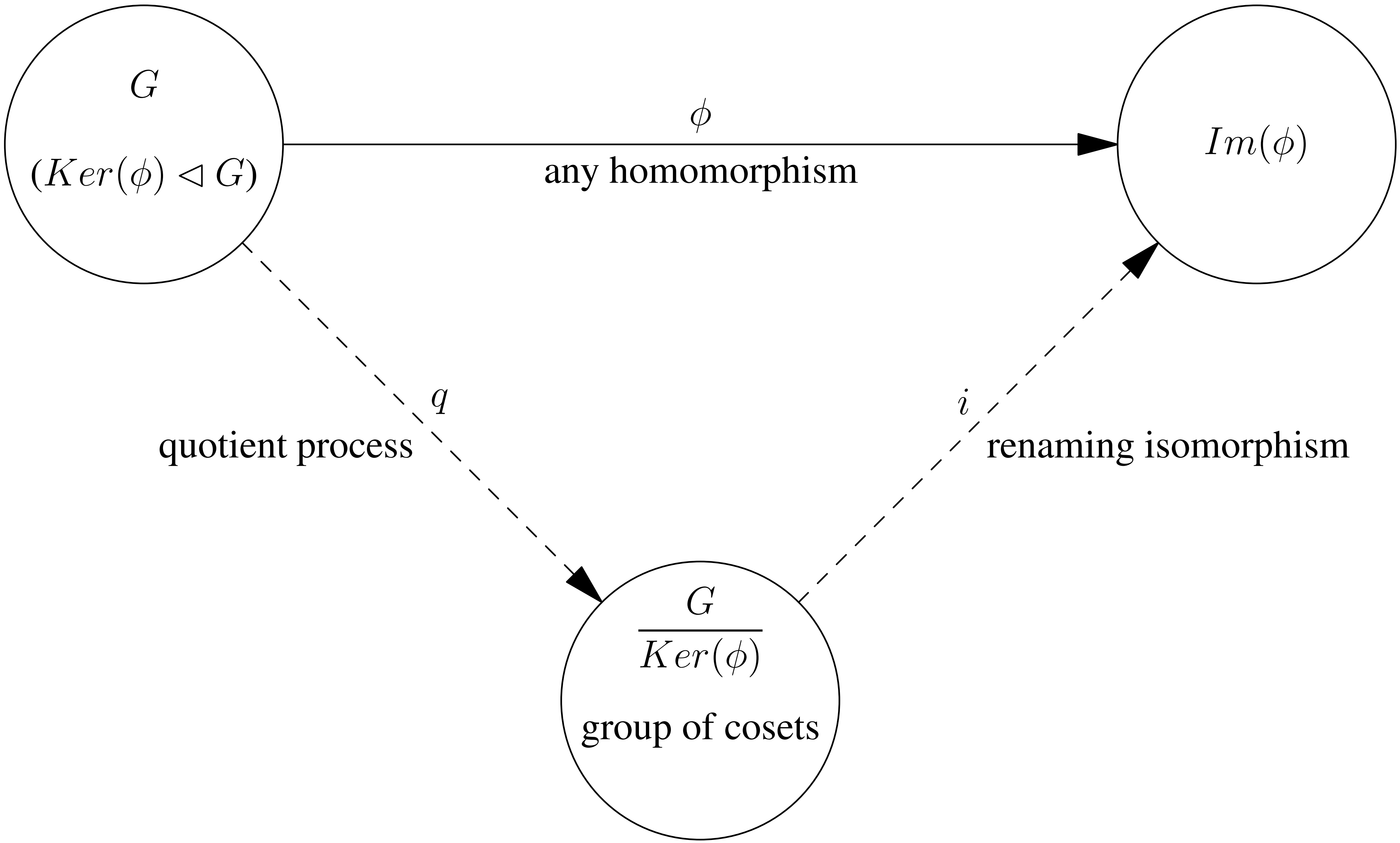


Homomorphisms

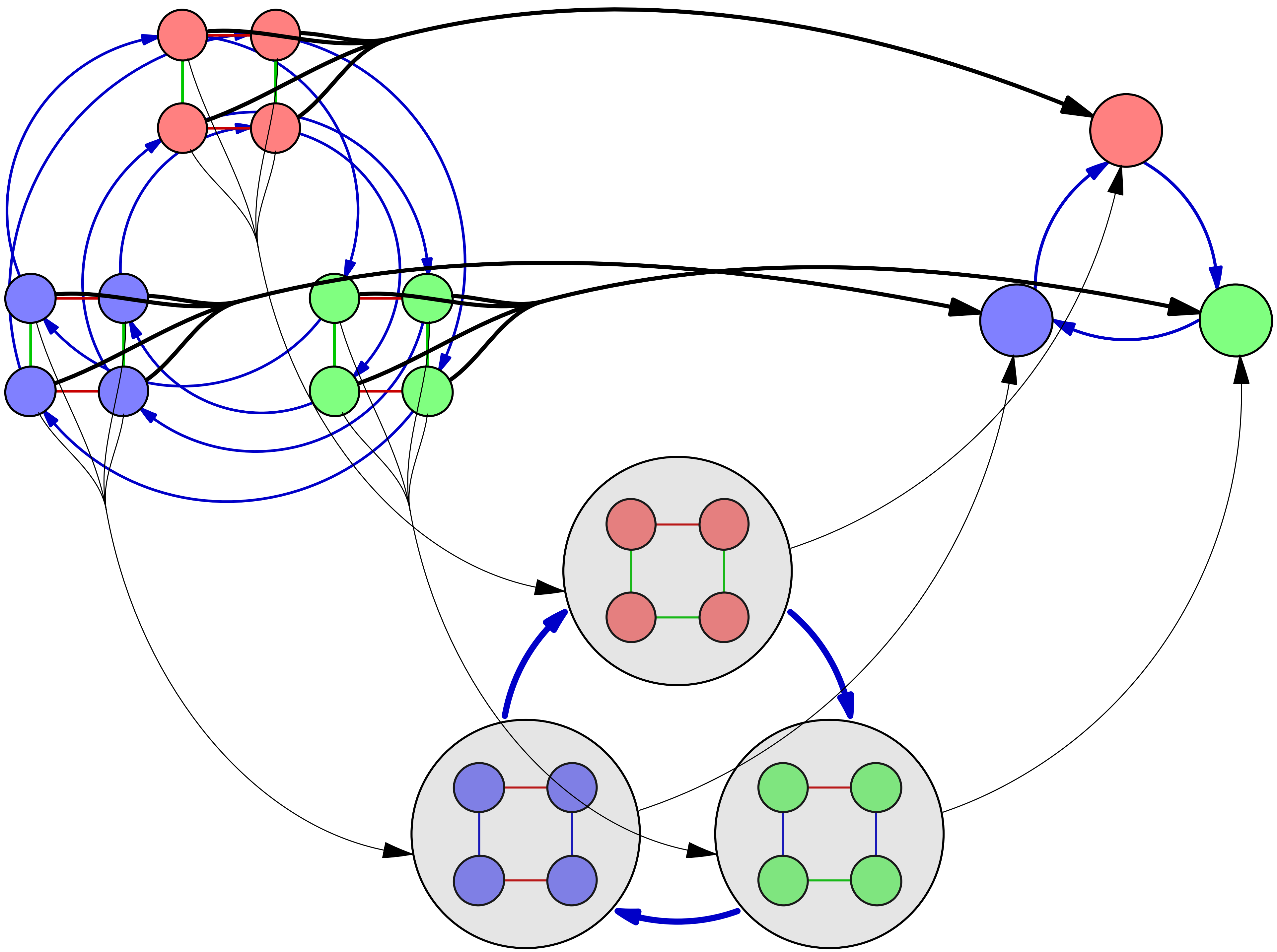
Example non-embedding, non-surjection



Homomorphisms



Homomorphisms

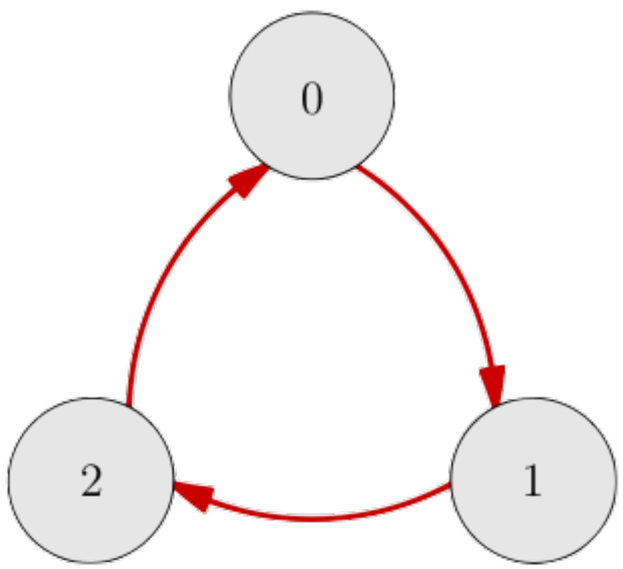


Are there non-Direct Products?

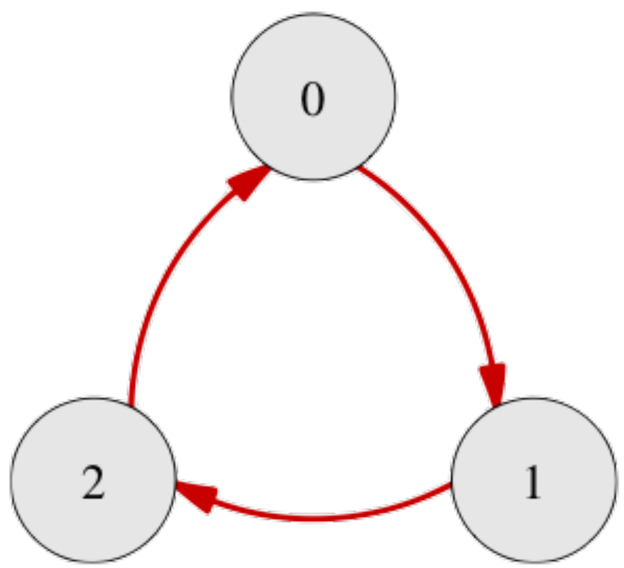
Are there non-Direct Products?

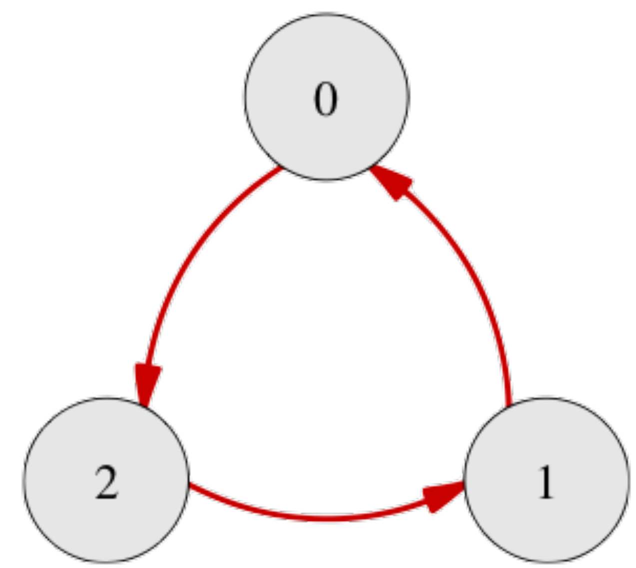
No more waiting!

Semidirect Products

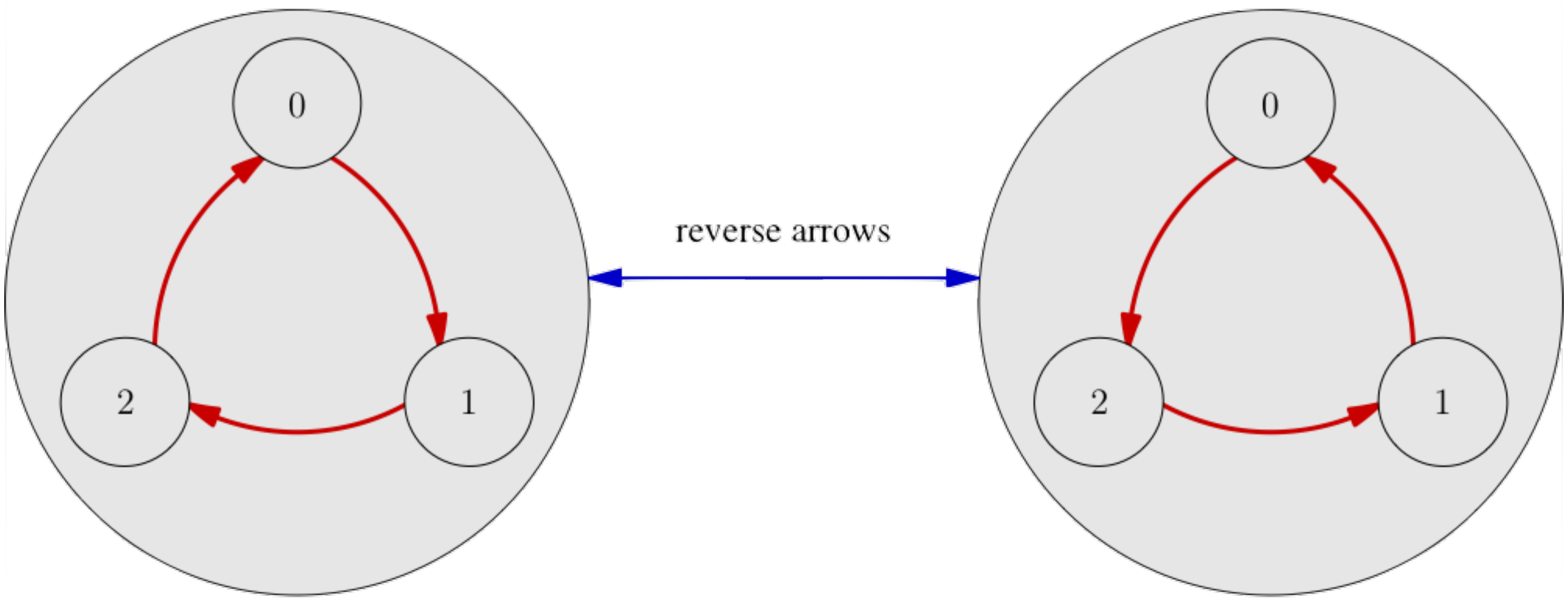


Semidirect Products

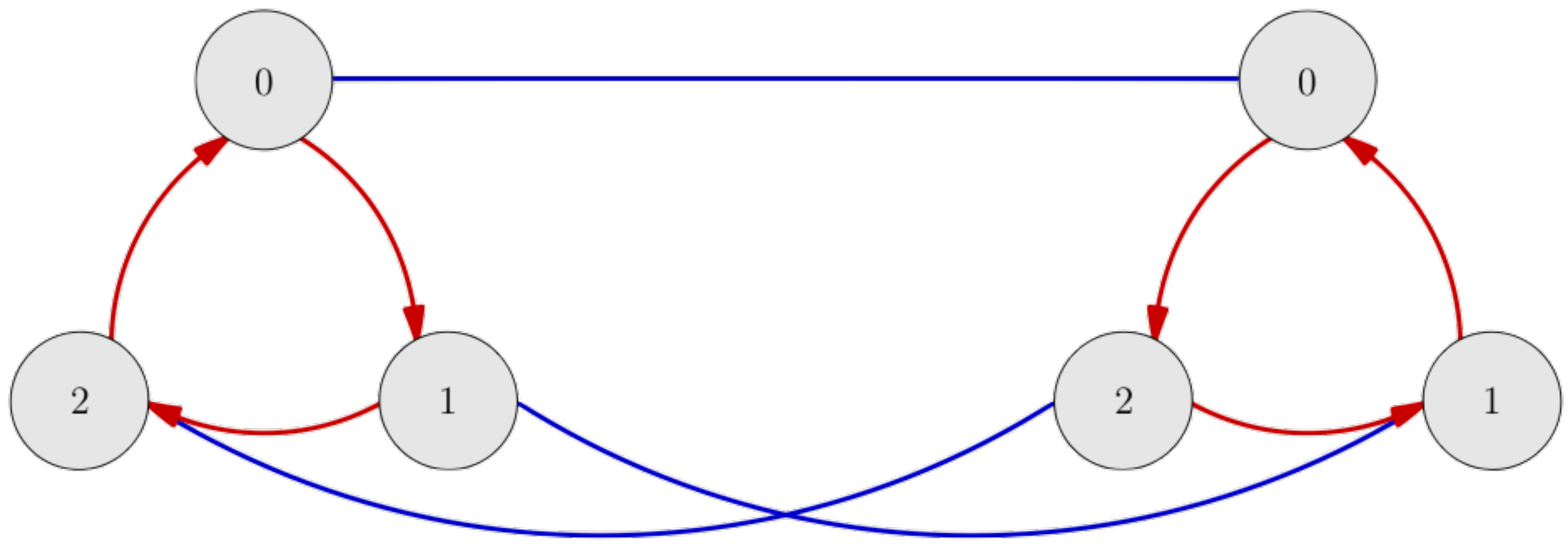




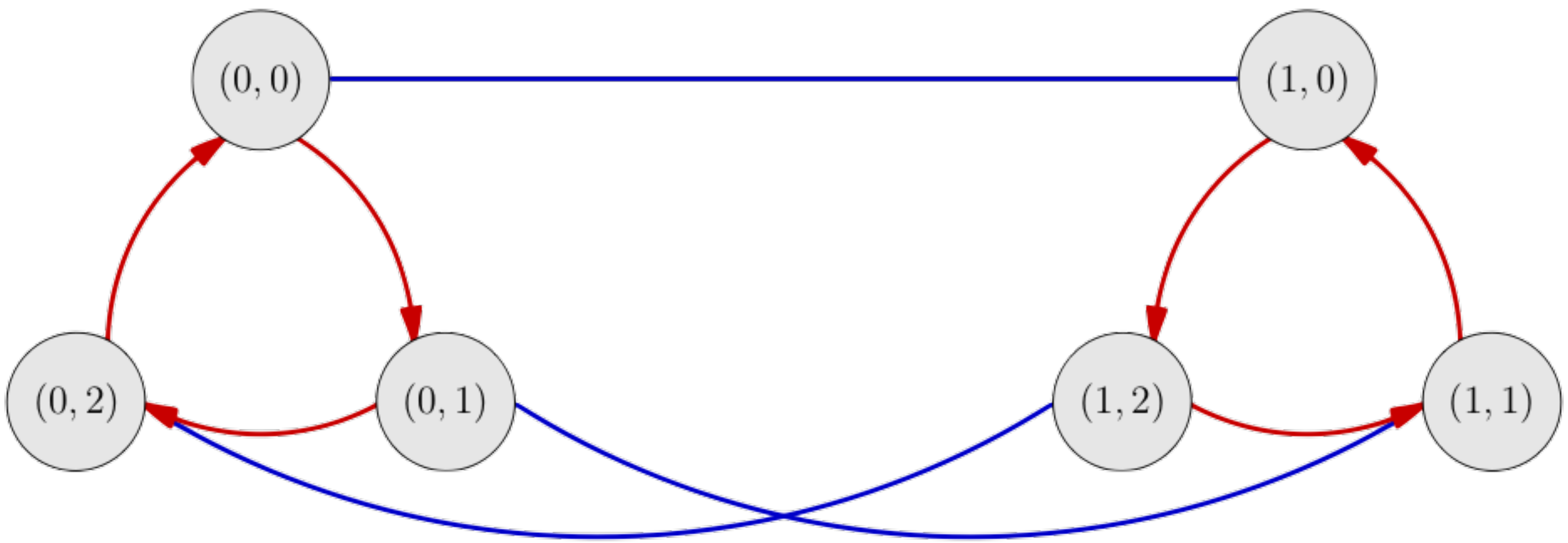
Semidirect Products



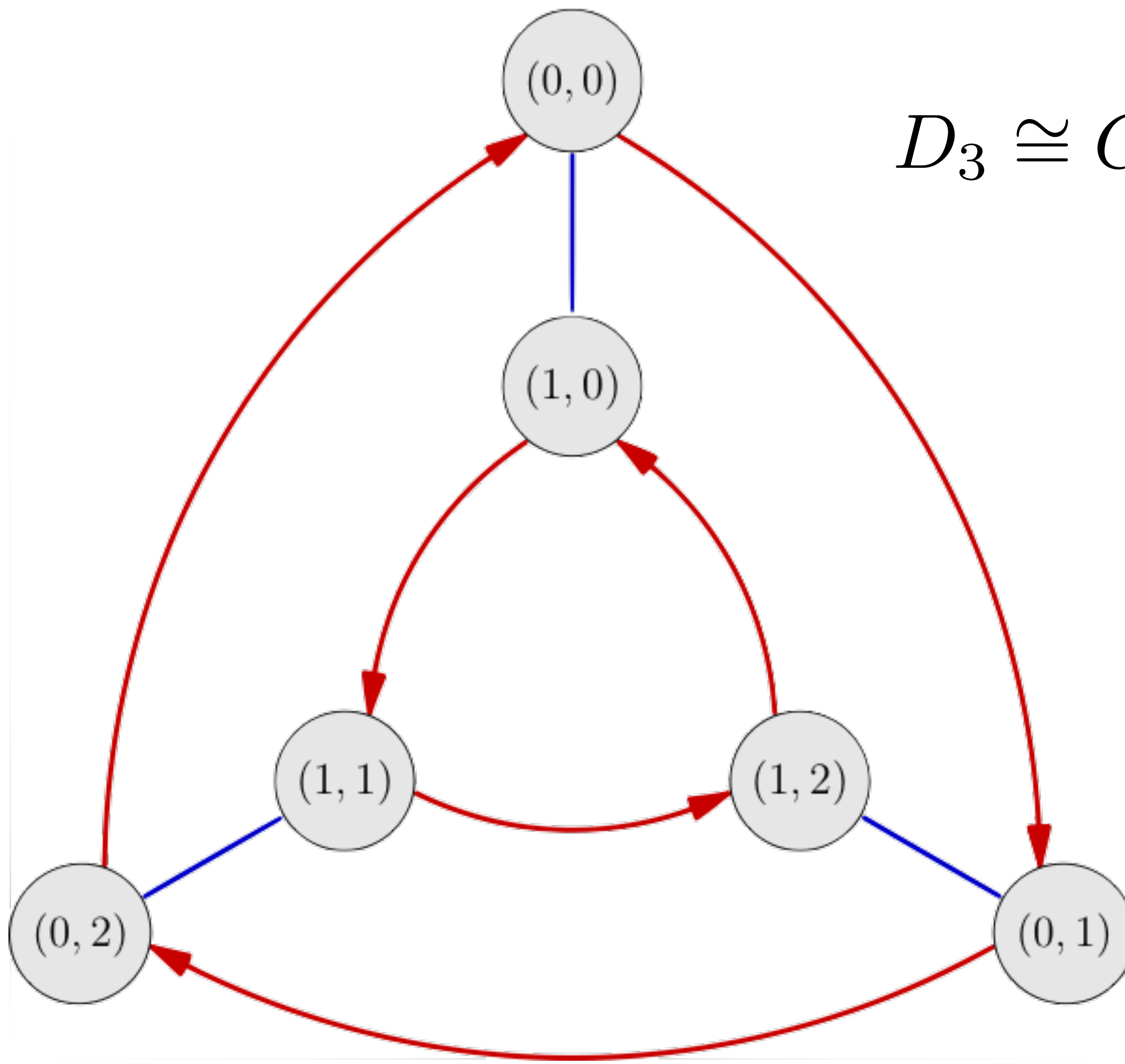
Semidirect Products



Semidirect Products

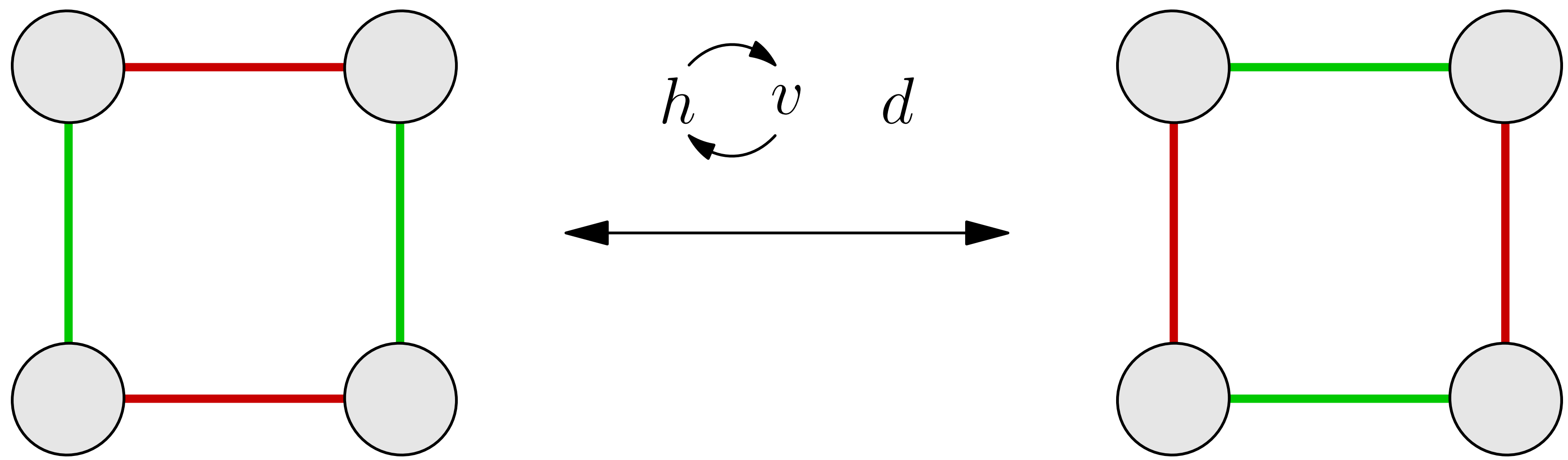


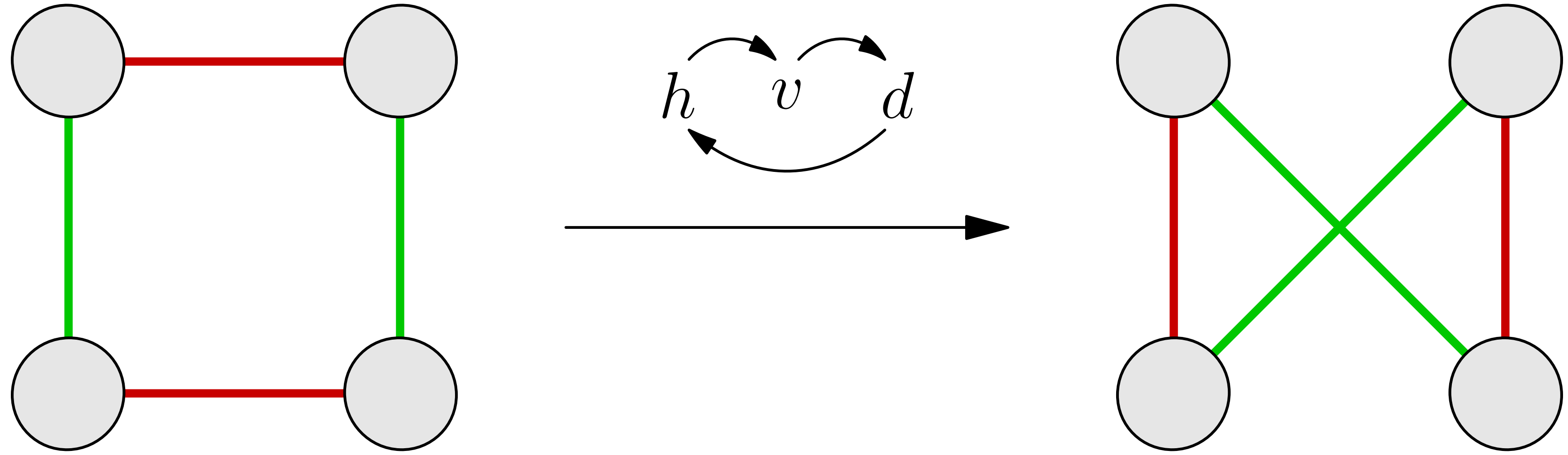
Semidirect Products



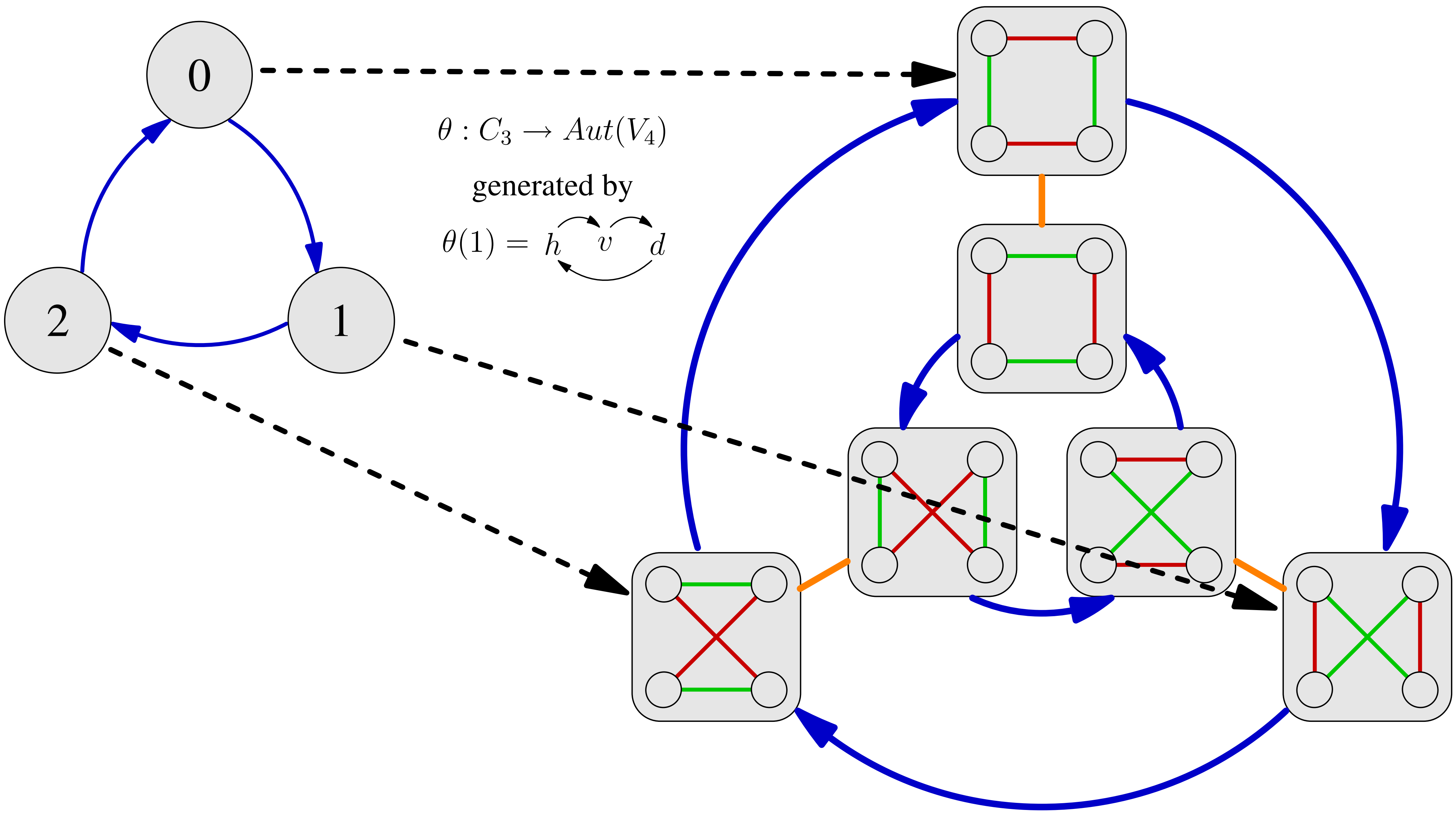
$$D_3 \cong C_3 \rtimes_\theta C_2$$

Semidirect Products

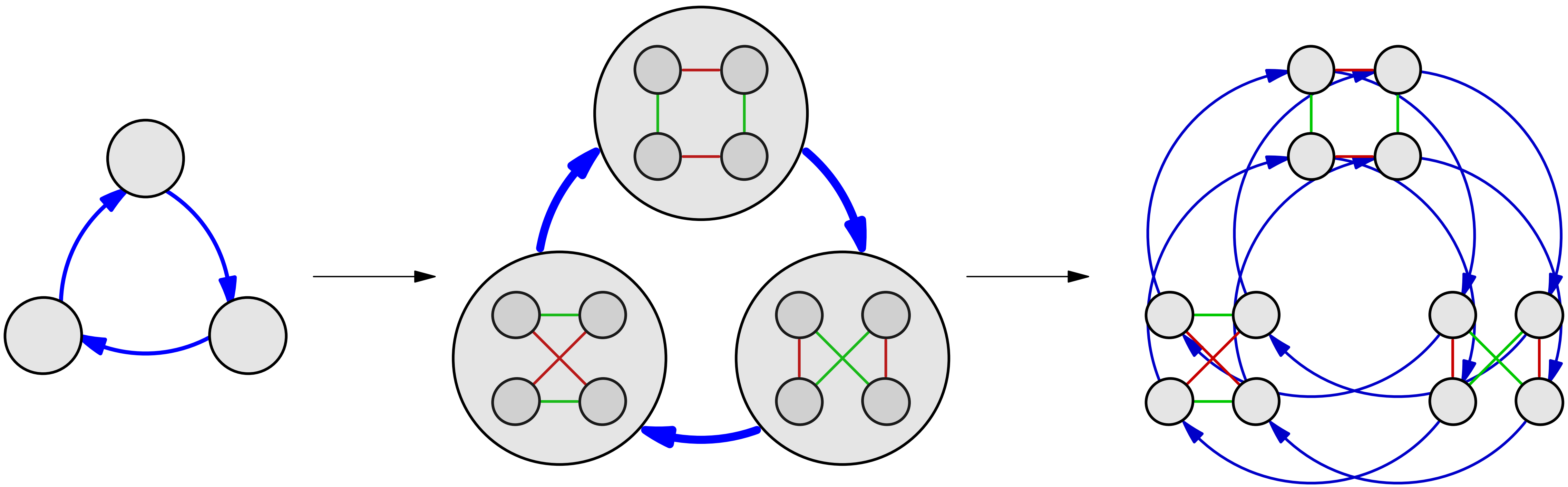




Semidirect Products



Semidirect Products

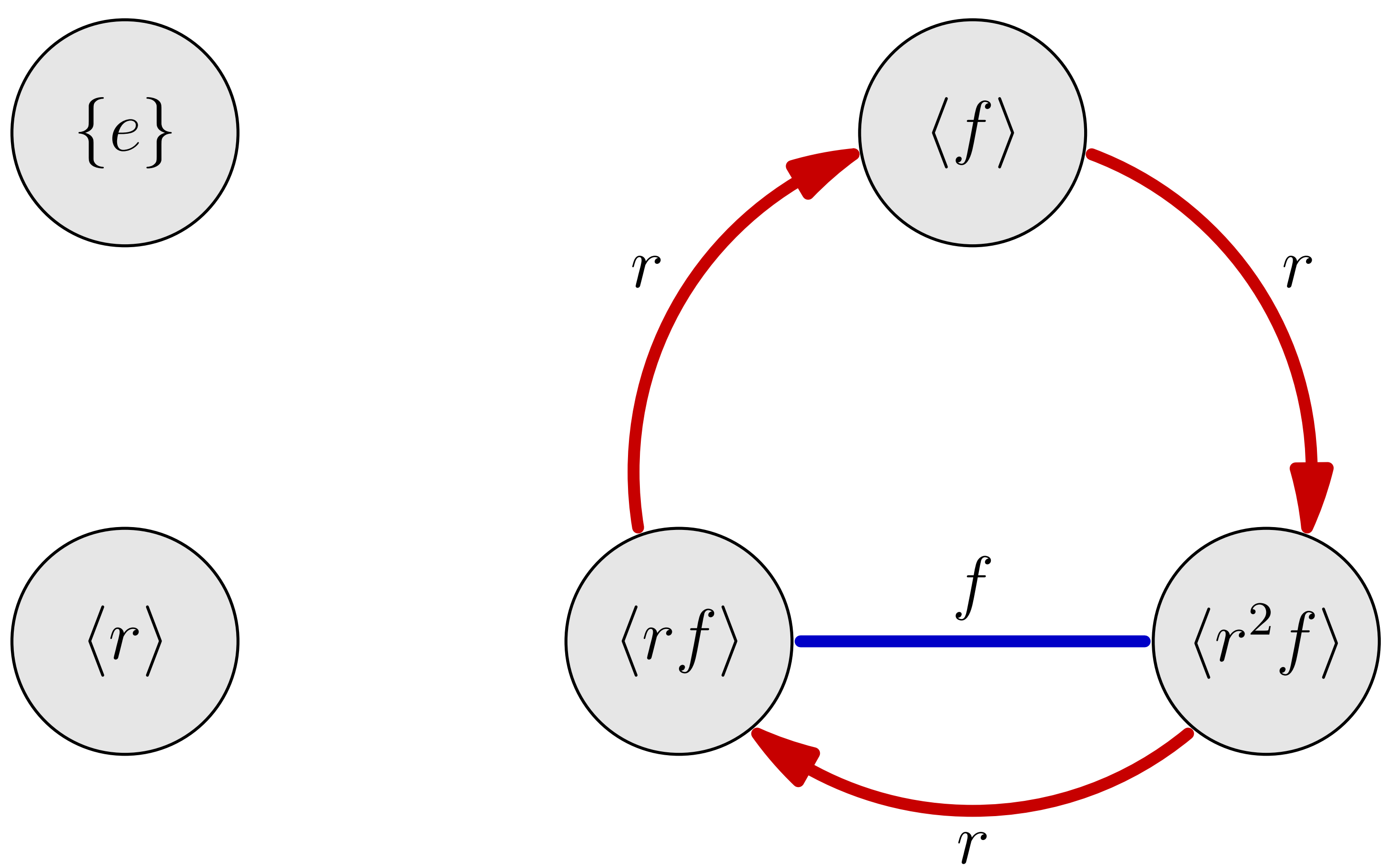


C_3 $\qquad$ $\theta(C_3) \subset Aut(V_4)$ $\qquad$ $A_4 \cong V_4 \rtimes_\theta C_3$

What groups are there?

Sylow Theory

- Cayley graphs generalize naturally to a group acting on any set of elements.
- E.g., here D_3 acts on its own subgroups by right multiplication.



Using Sylow Theory

Classifying the groups of order 8

- The Fundamental Theorem of Abelian Groups tells us that the following groups exist.

$$C_8 \qquad\qquad C_4 \times C_2 \qquad\qquad C_2 \times C_2 \times C_2$$

- The nonabelian cases are the interesting ones.

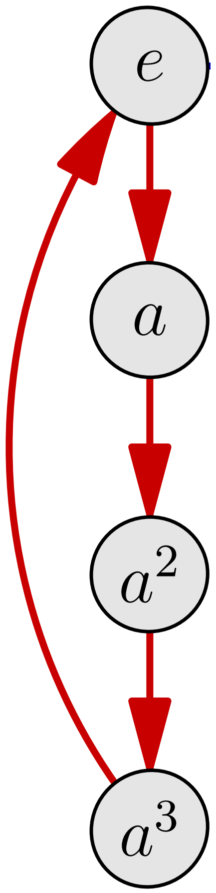
Using Sylow Theory

Classifying the groups of order 8

- First Sylow Theorem:
  There is a subgroup of order 4.
- Previous classifications: It must be C_4 or V_4.
- If it were V_4, we would have only elements of order 2, and thus the group would be abelian.

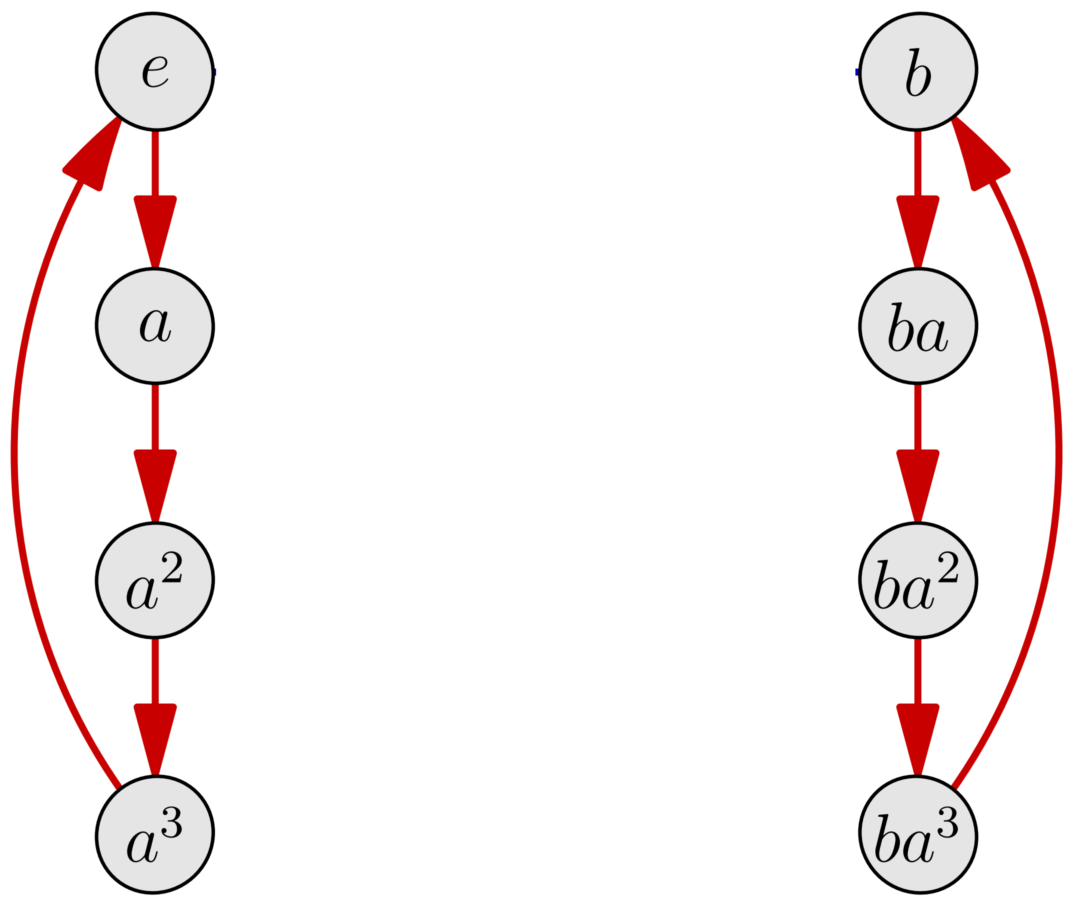
Using Sylow Theory

Classifying the groups of order 8



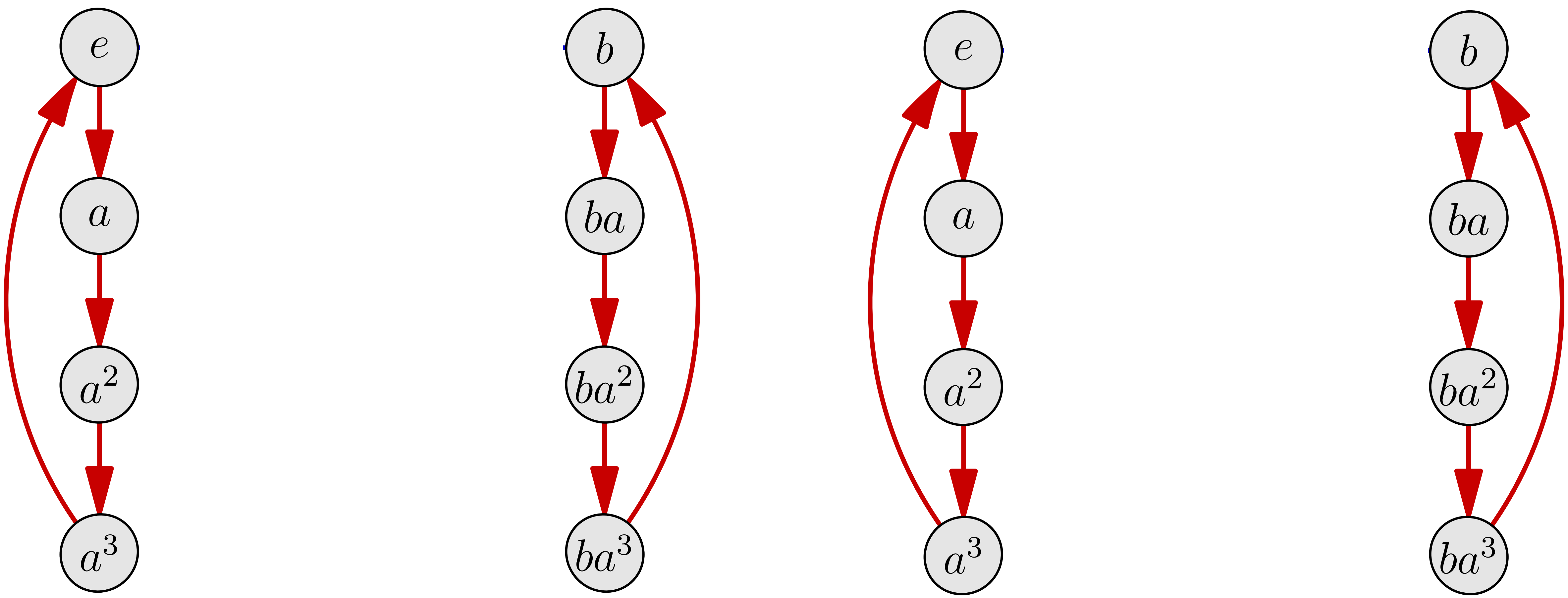
Using Sylow Theory

Classifying the groups of order 8



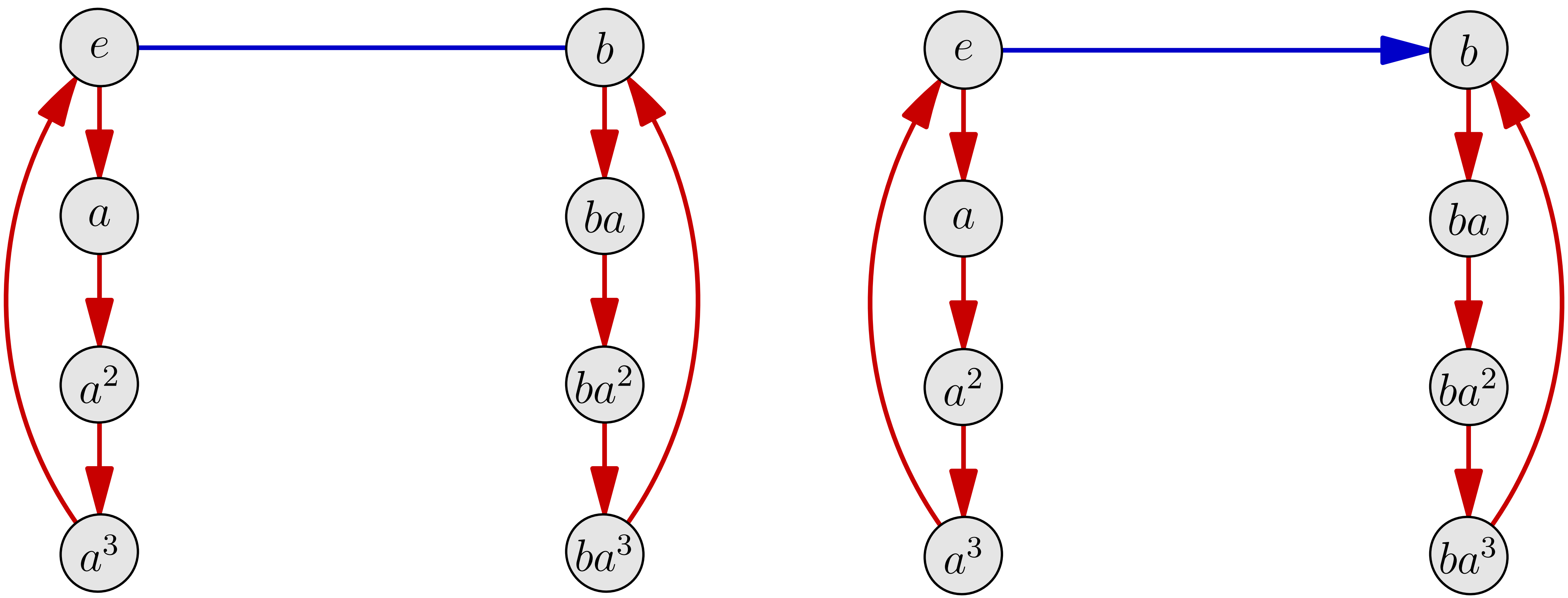
Using Sylow Theory

Classifying the groups of order 8



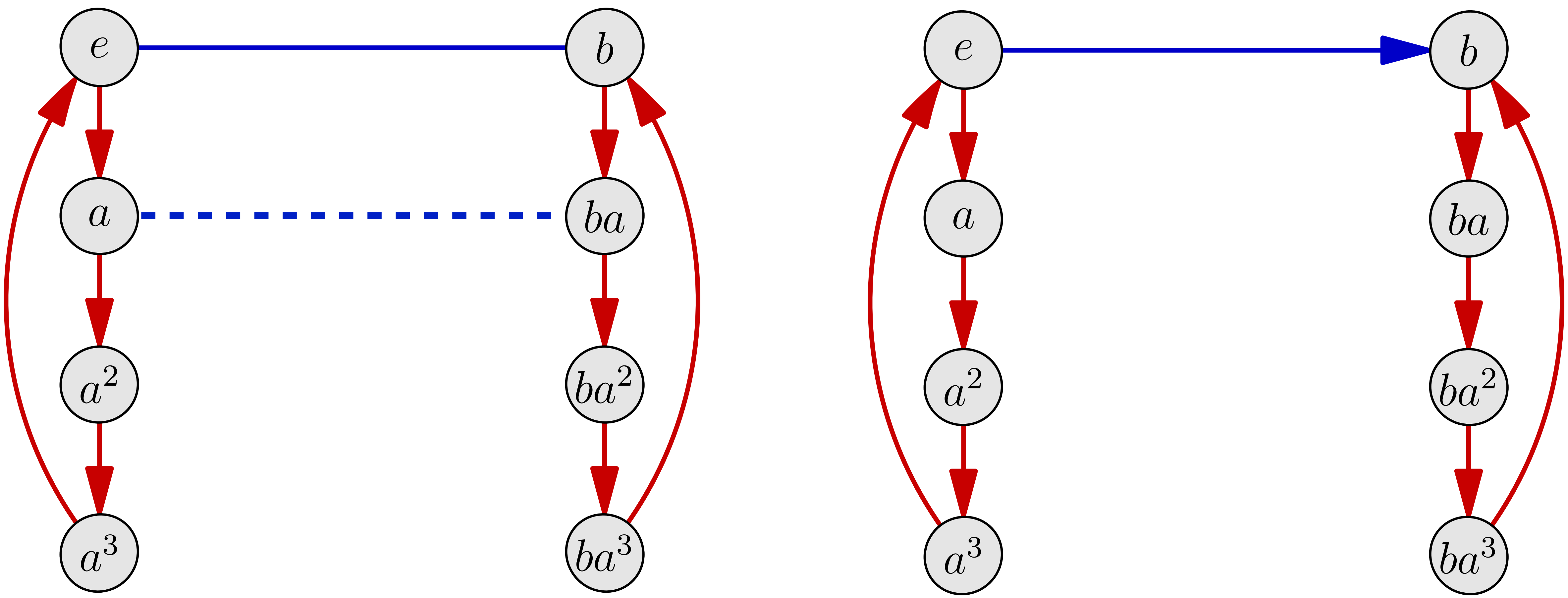
Using Sylow Theory

Classifying the groups of order 8



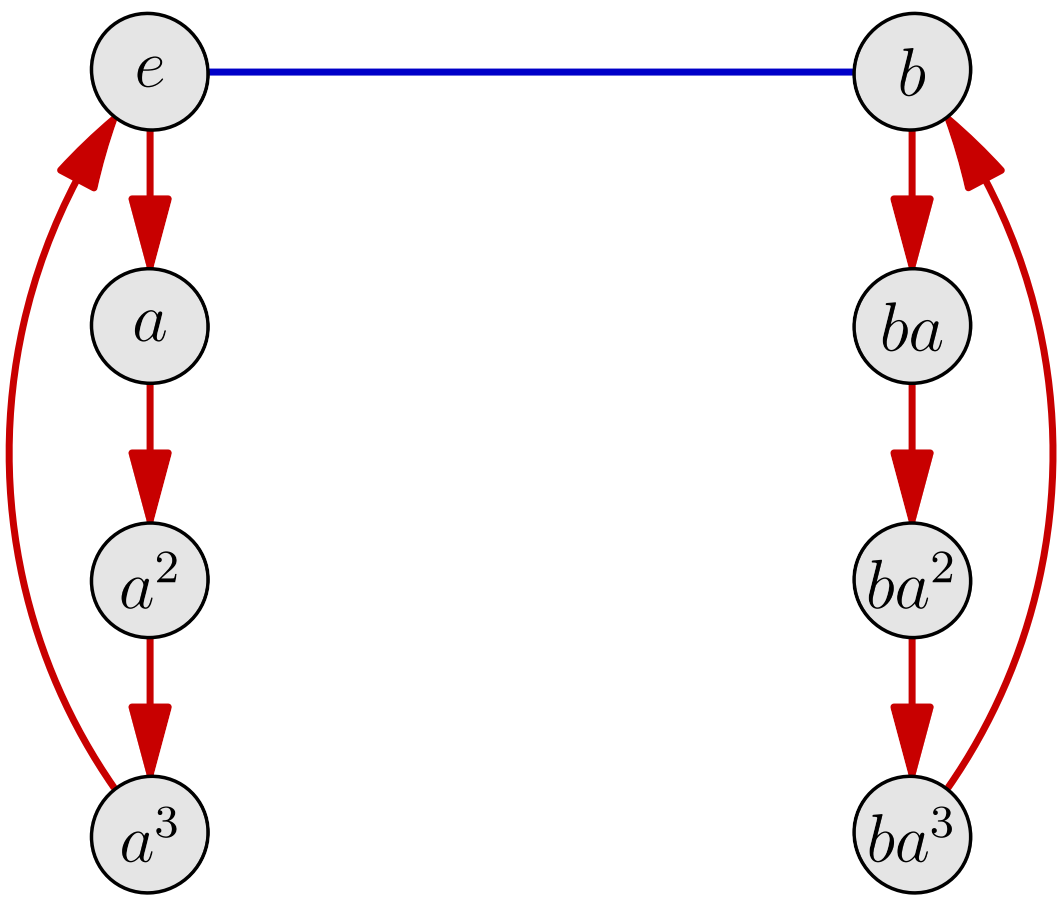
Using Sylow Theory

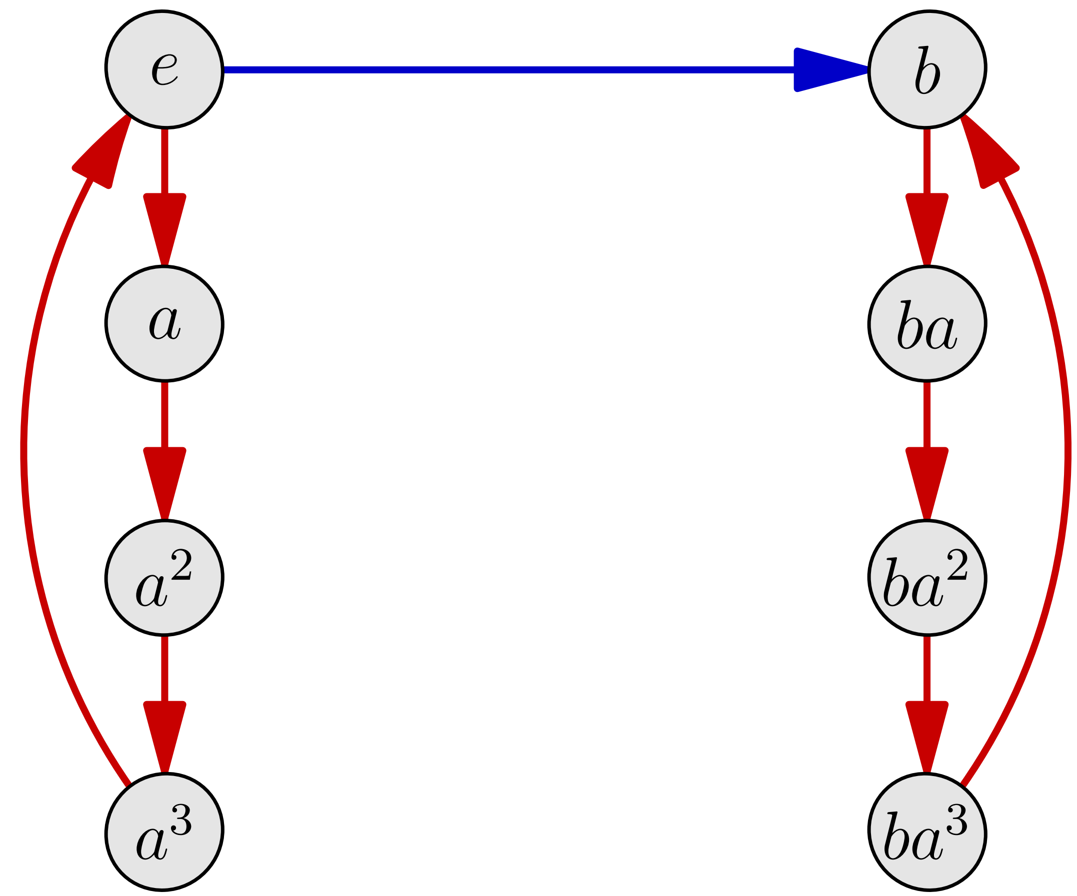
Classifying the groups of order 8



Using Sylow Theory

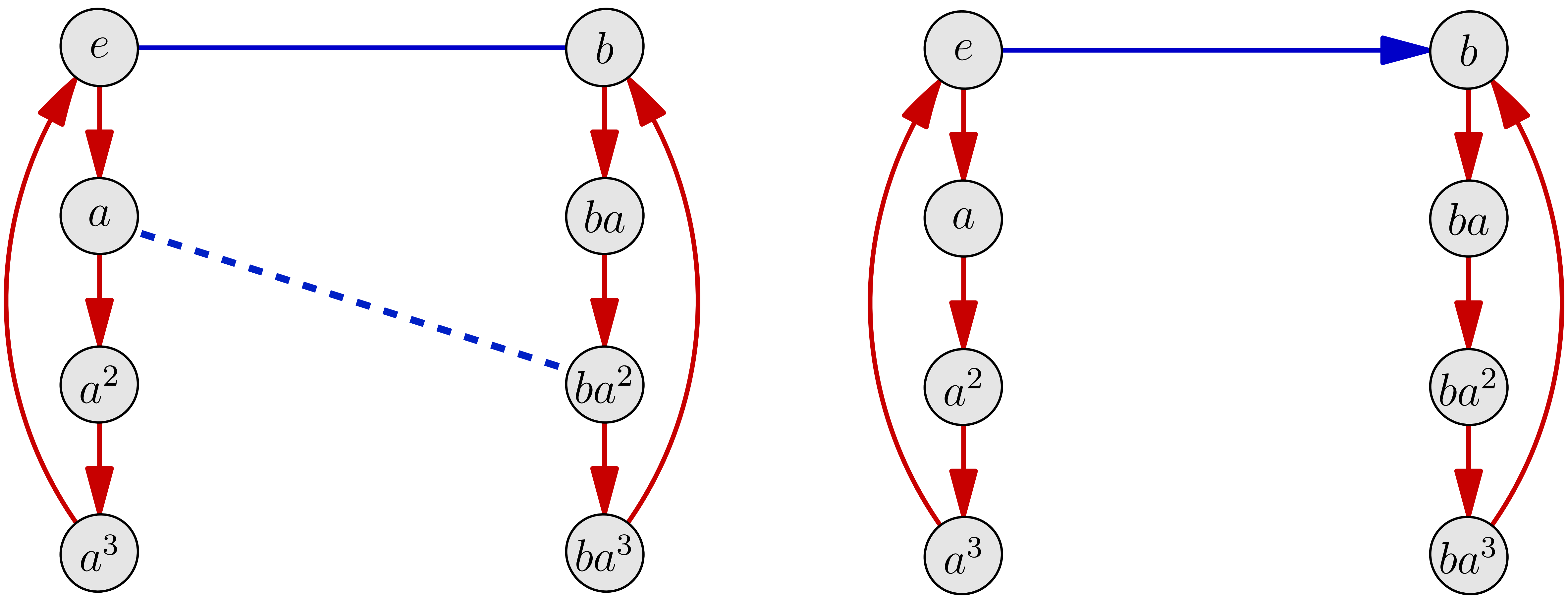
Classifying the groups of order 8





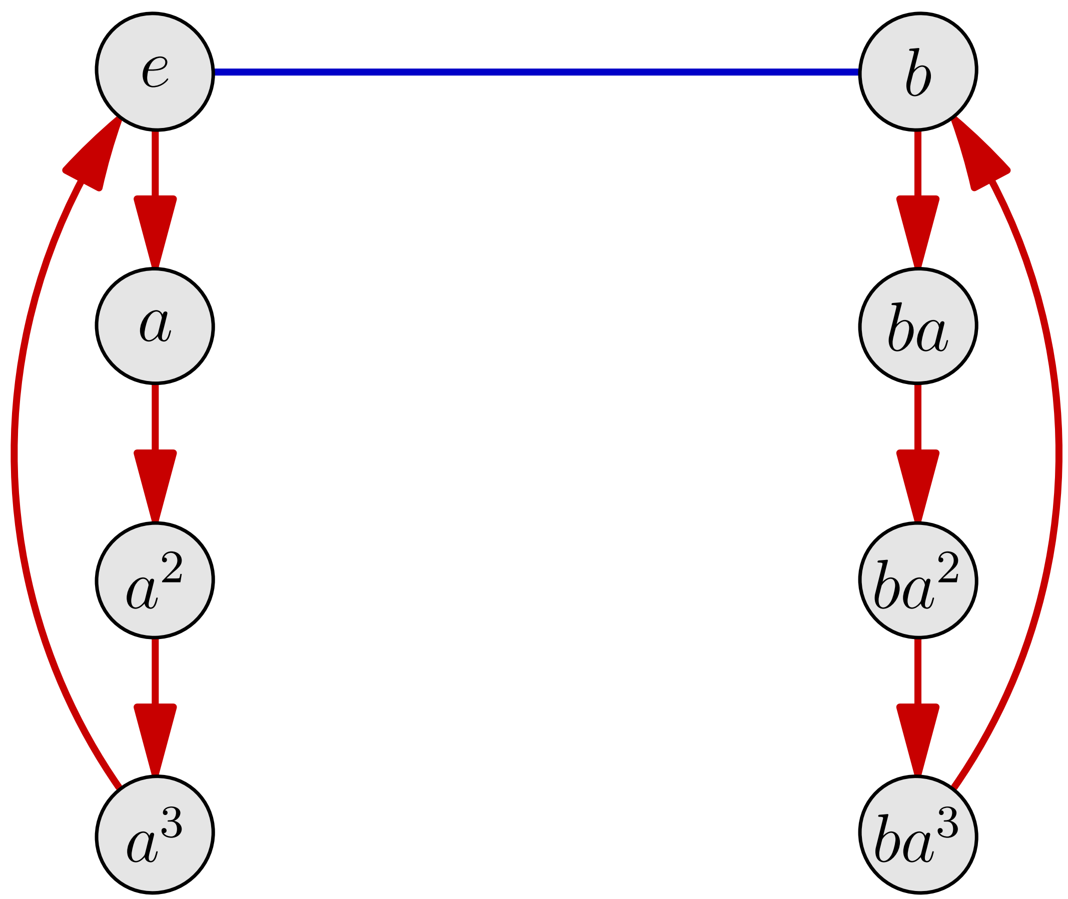
Using Sylow Theory

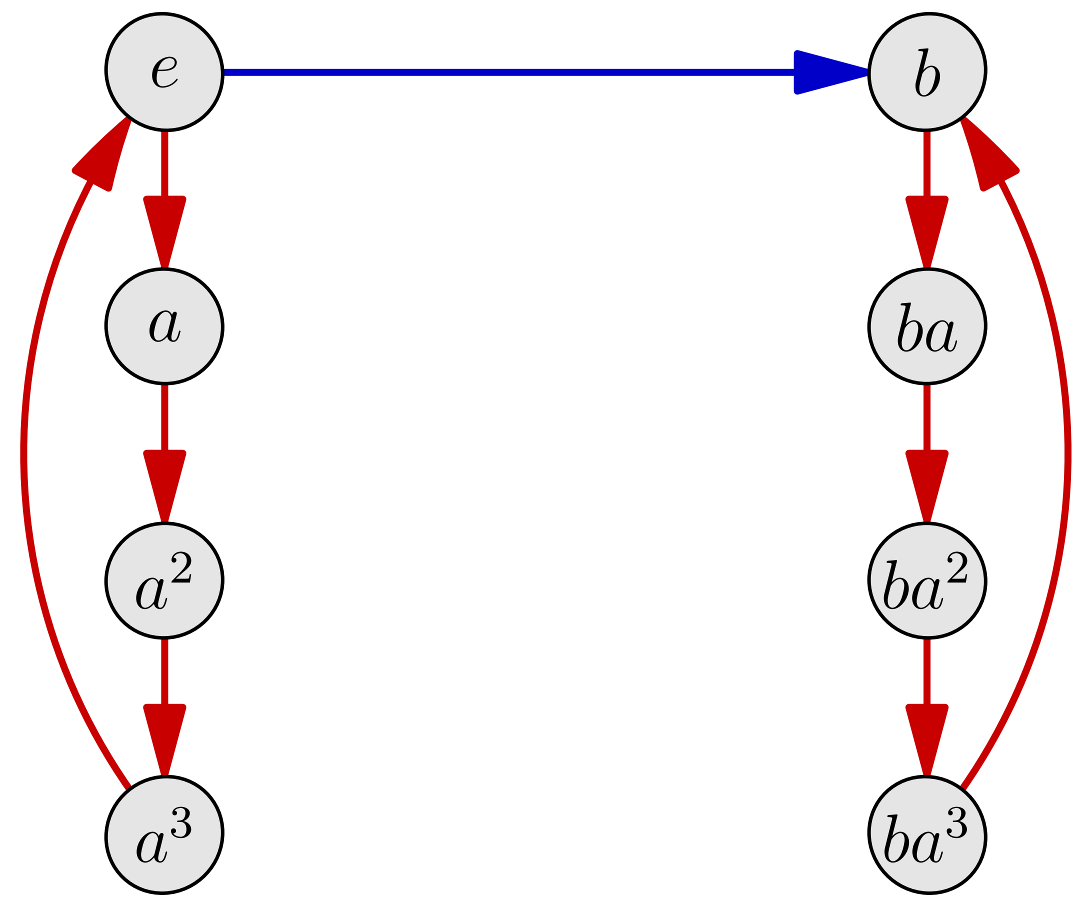
Classifying the groups of order 8



Using Sylow Theory

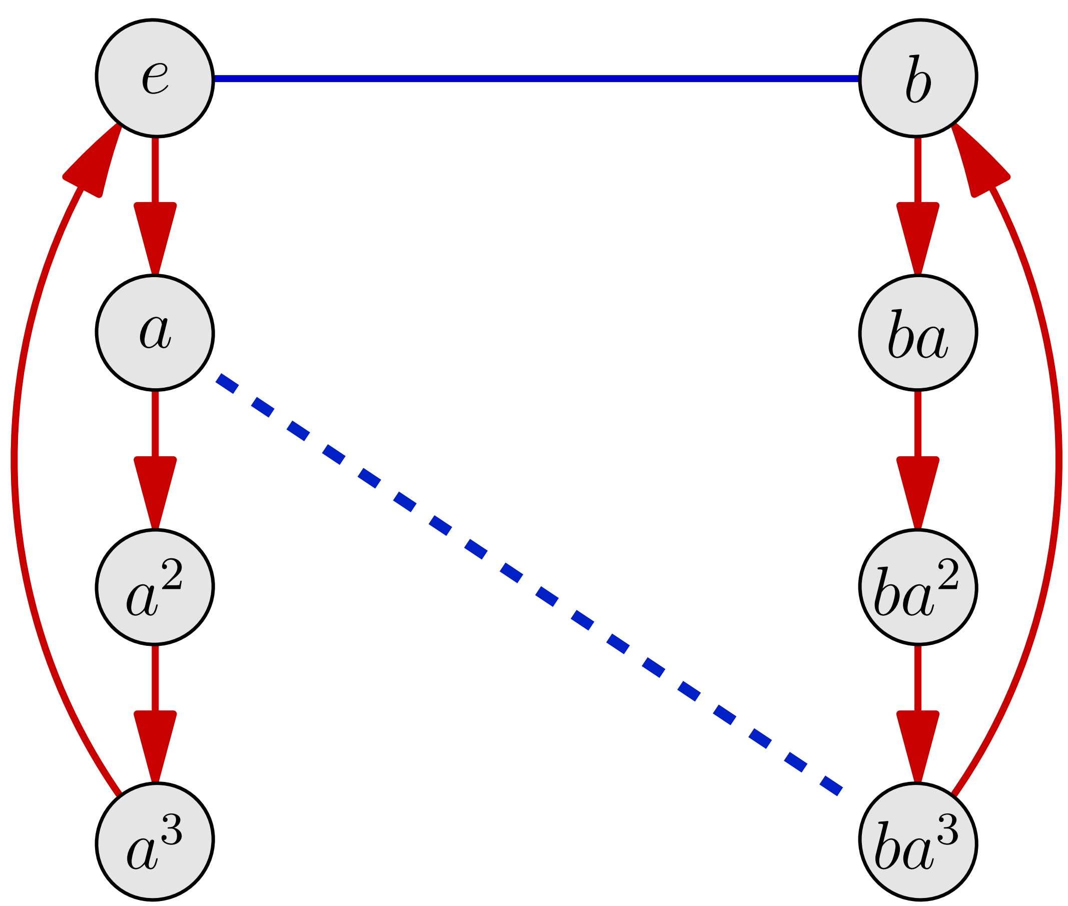
Classifying the groups of order 8

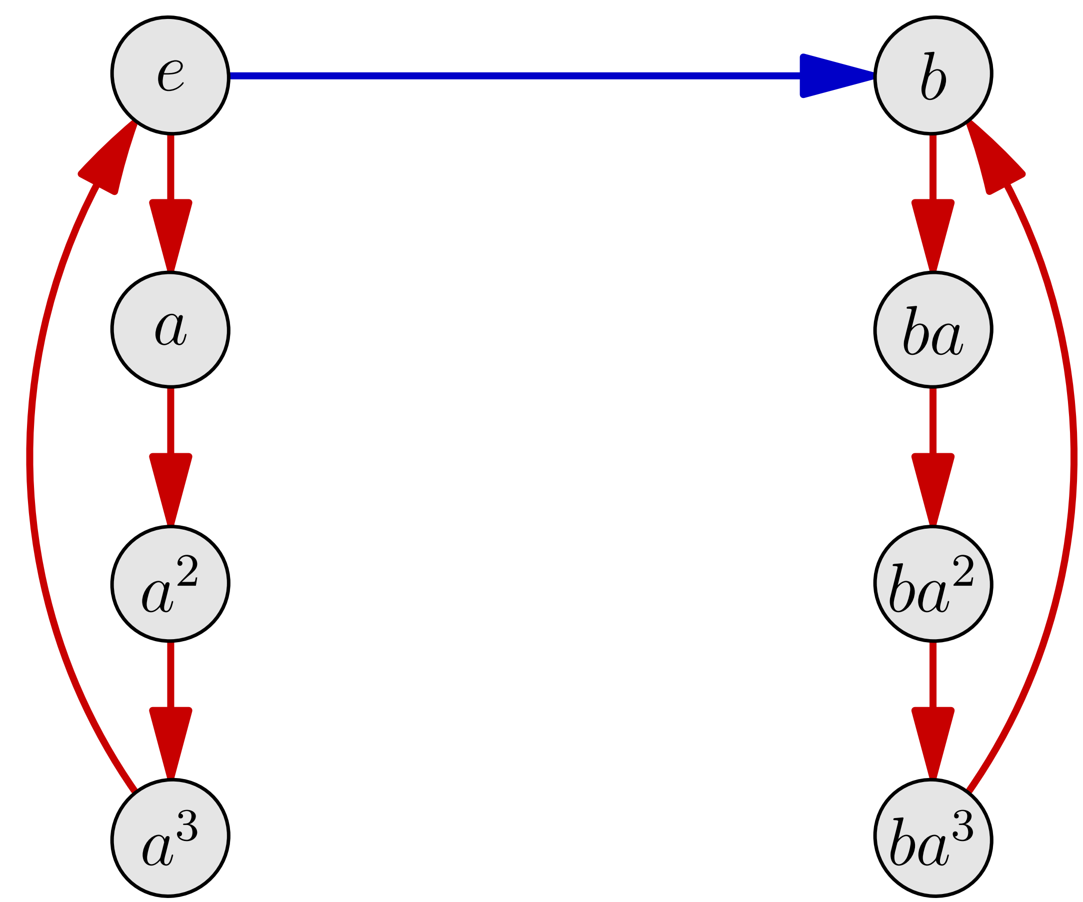




Using Sylow Theory

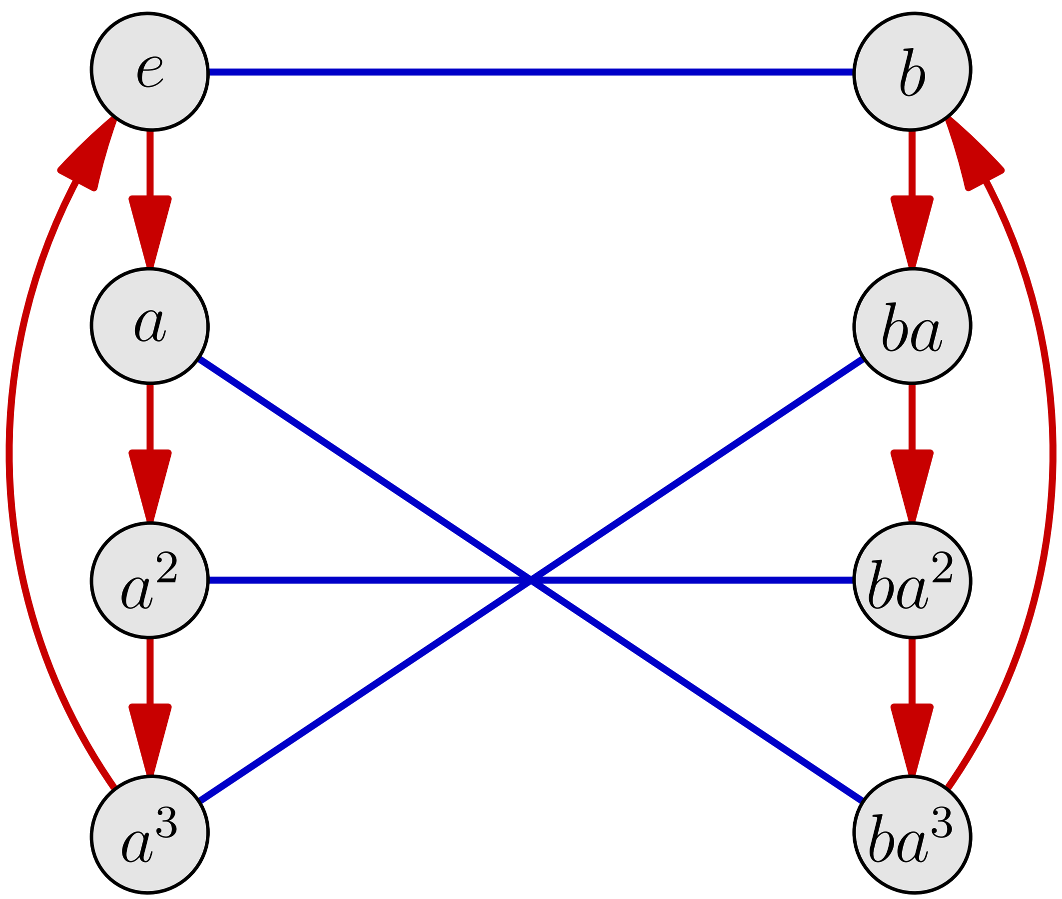
Classifying the groups of order 8

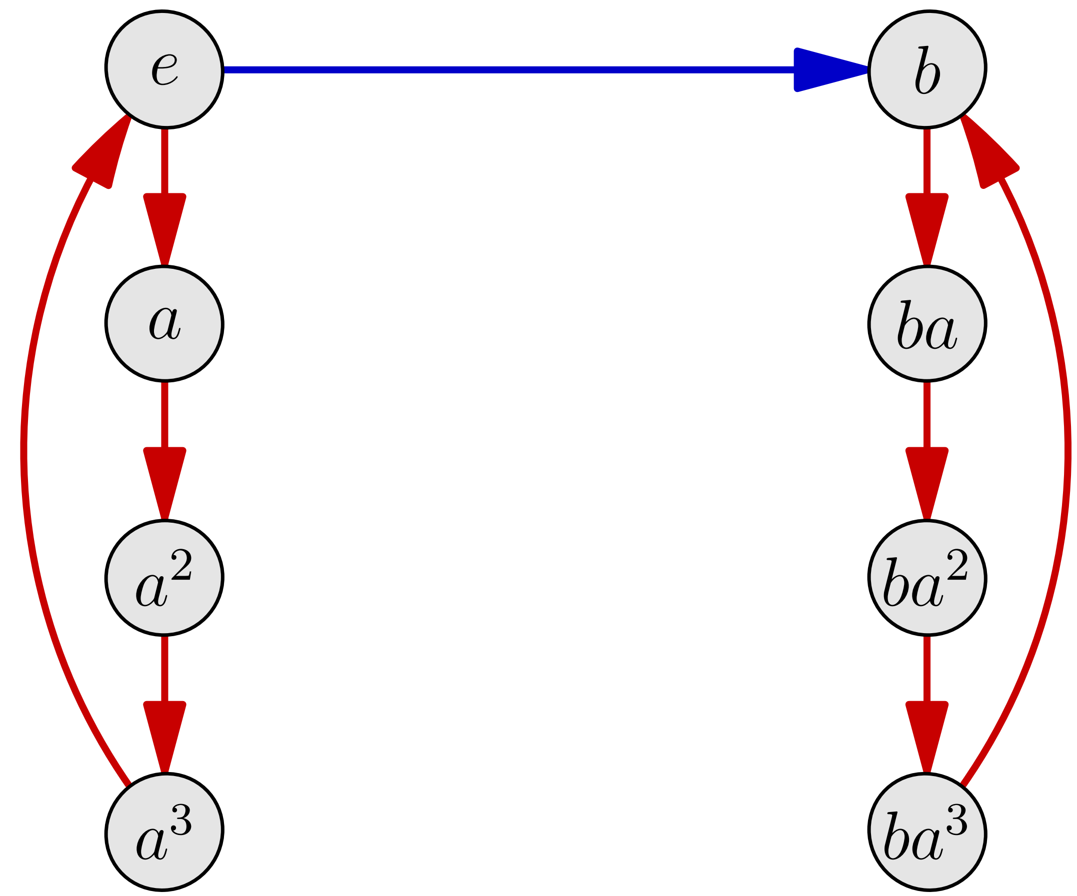




Using Sylow Theory

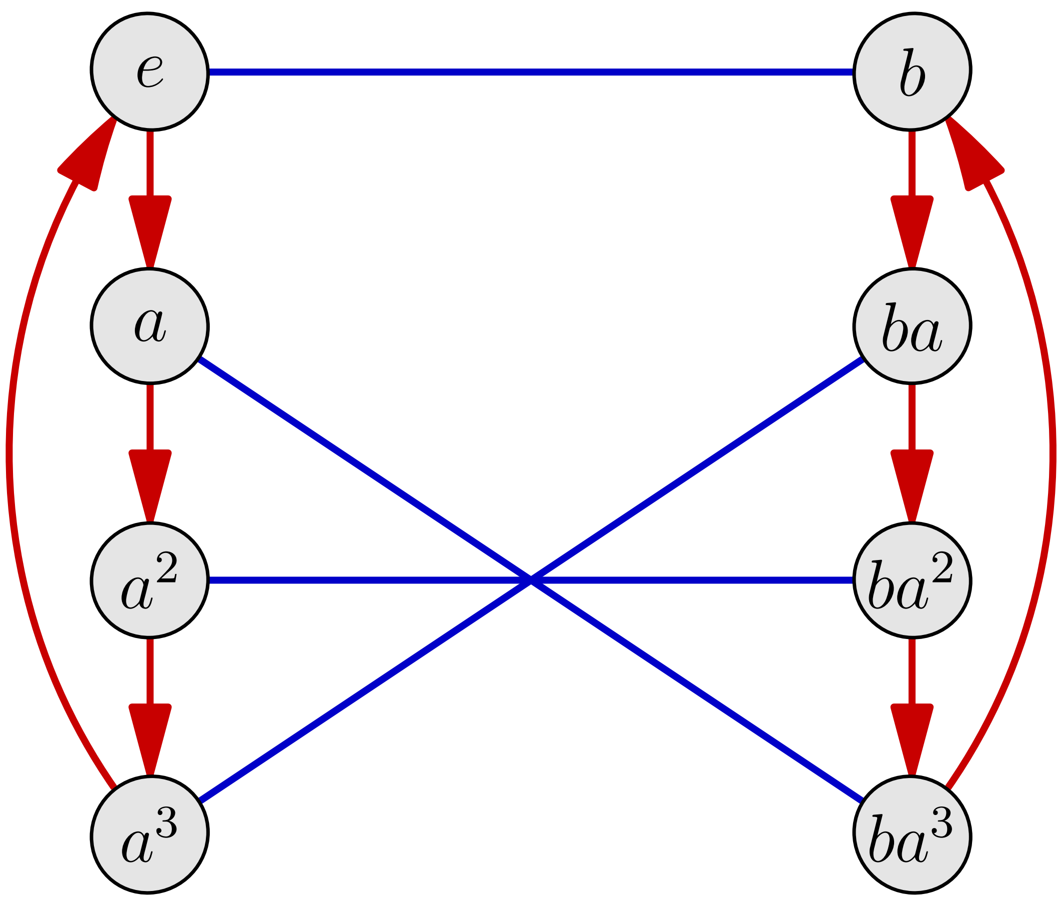
Classifying the groups of order 8

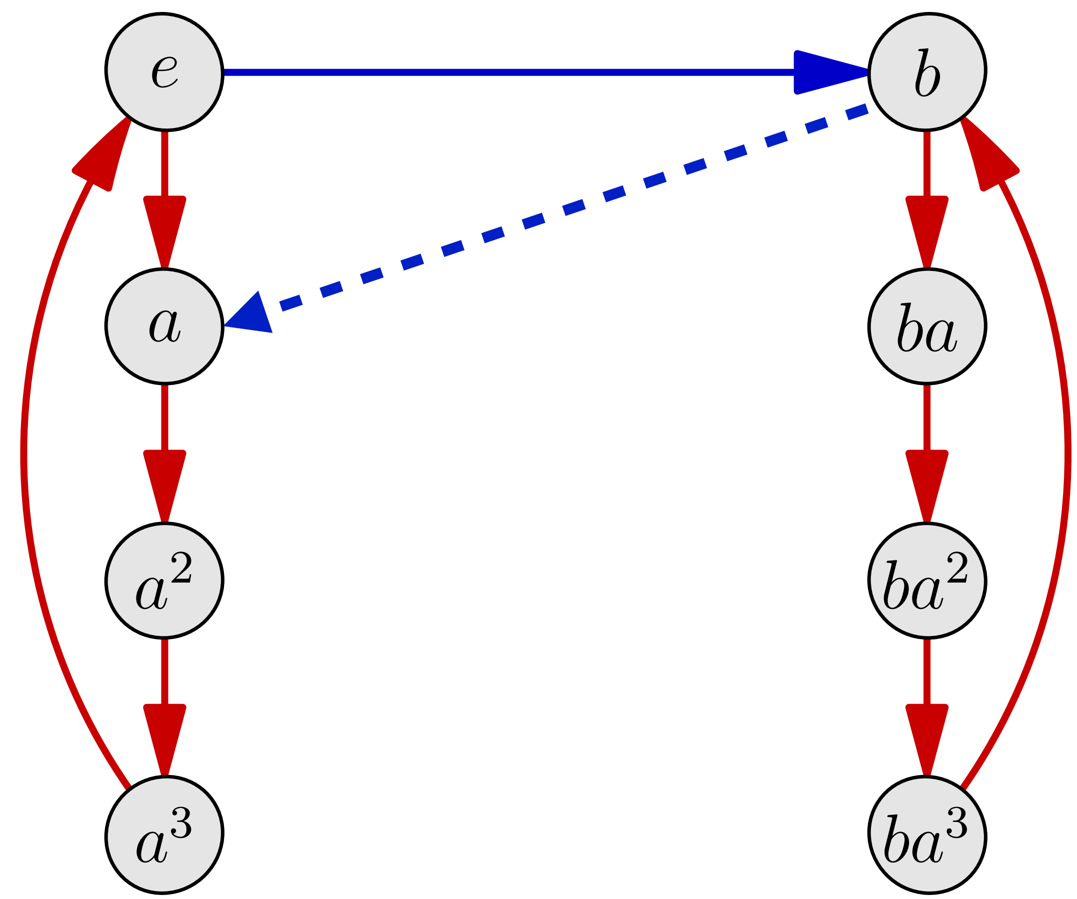




Using Sylow Theory

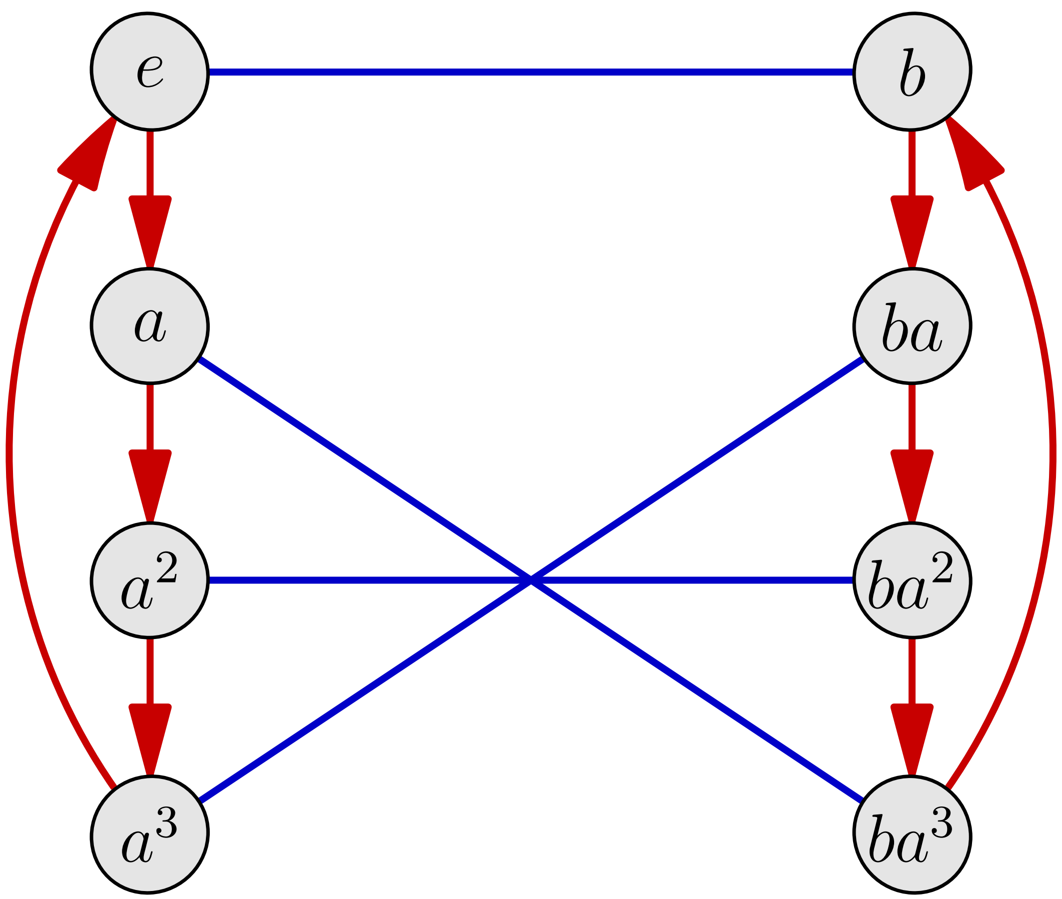
Classifying the groups of order 8

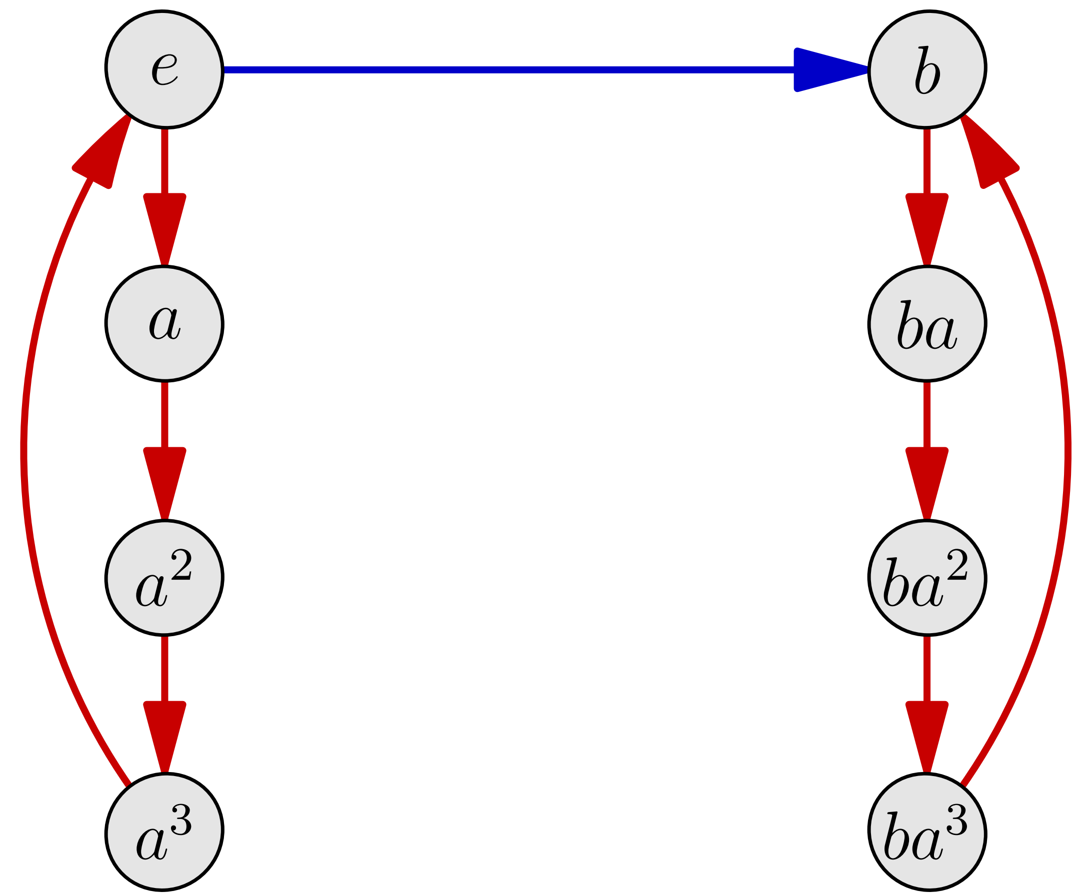




Using Sylow Theory

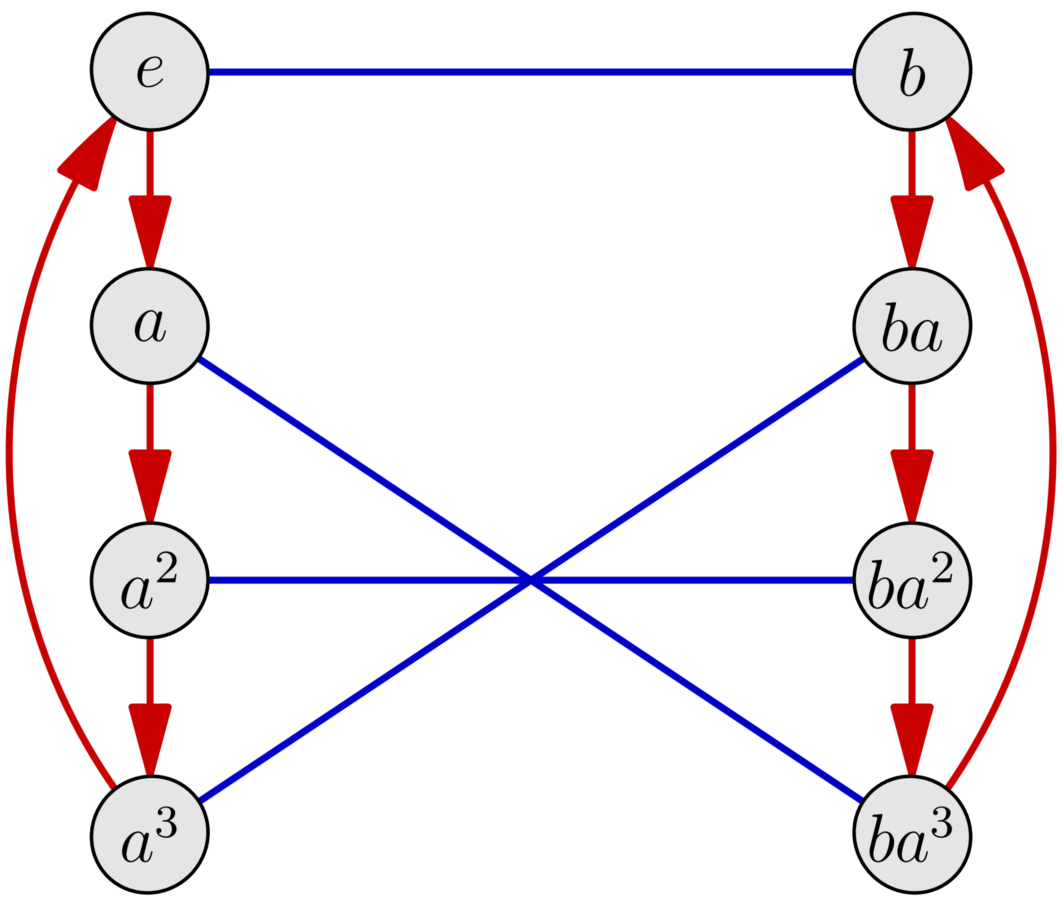
Classifying the groups of order 8

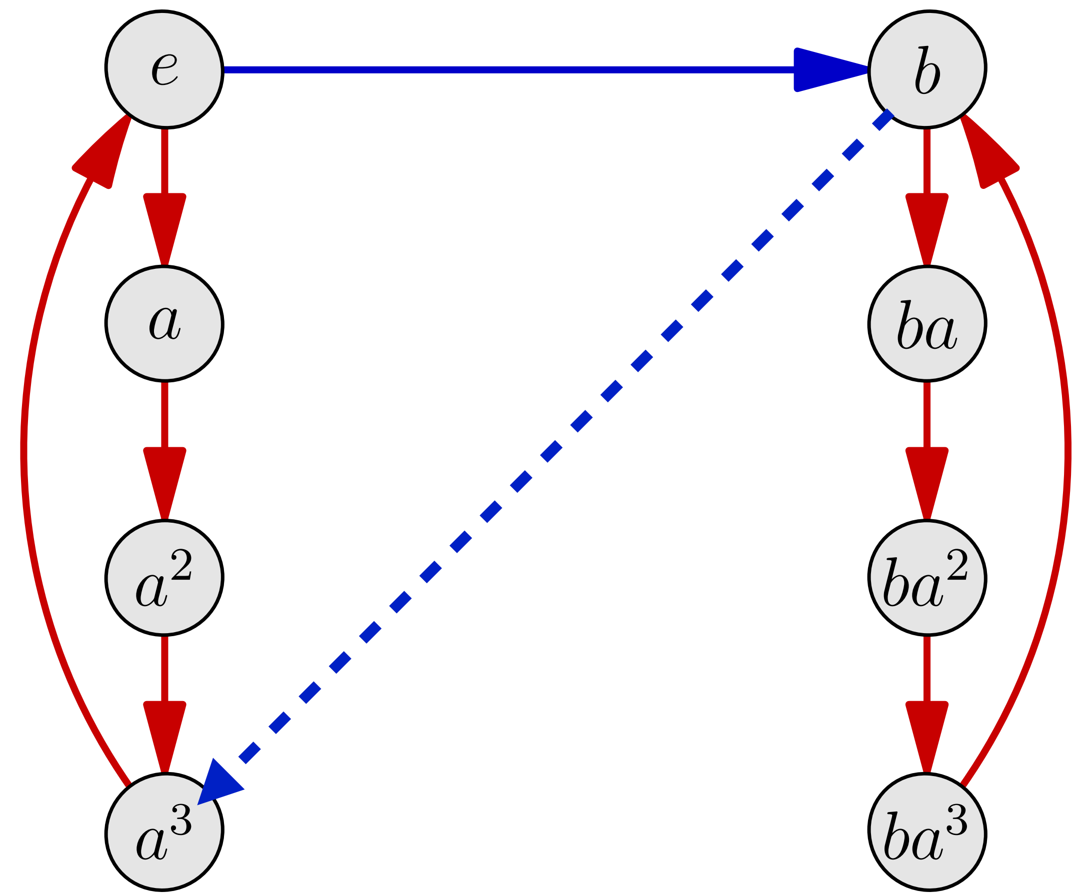




Using Sylow Theory

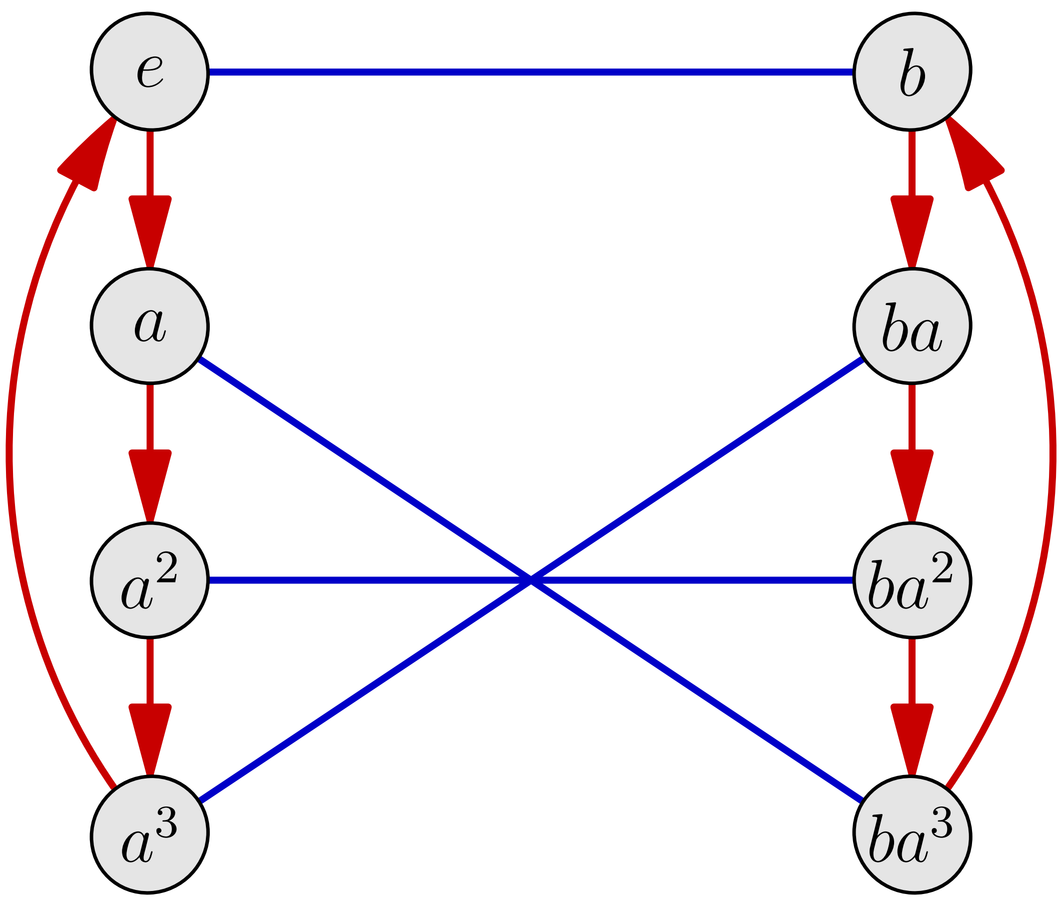
Classifying the groups of order 8

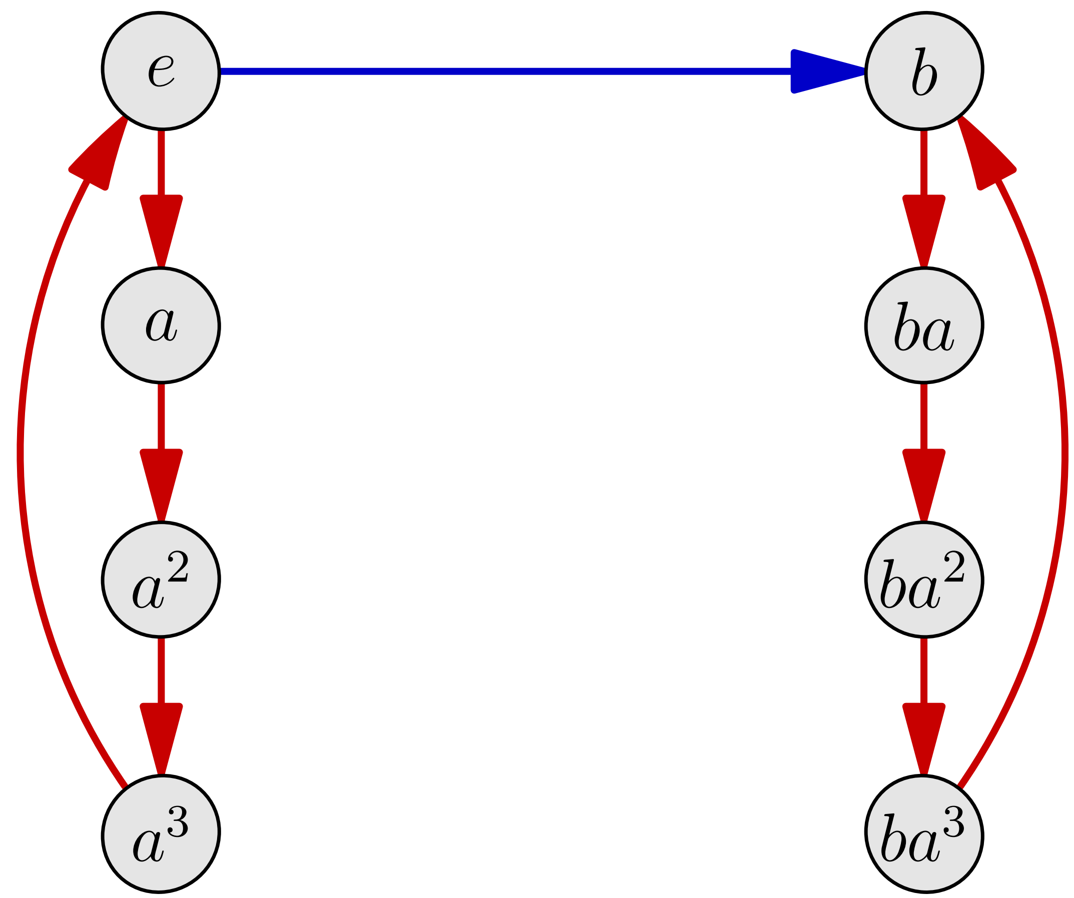




Using Sylow Theory

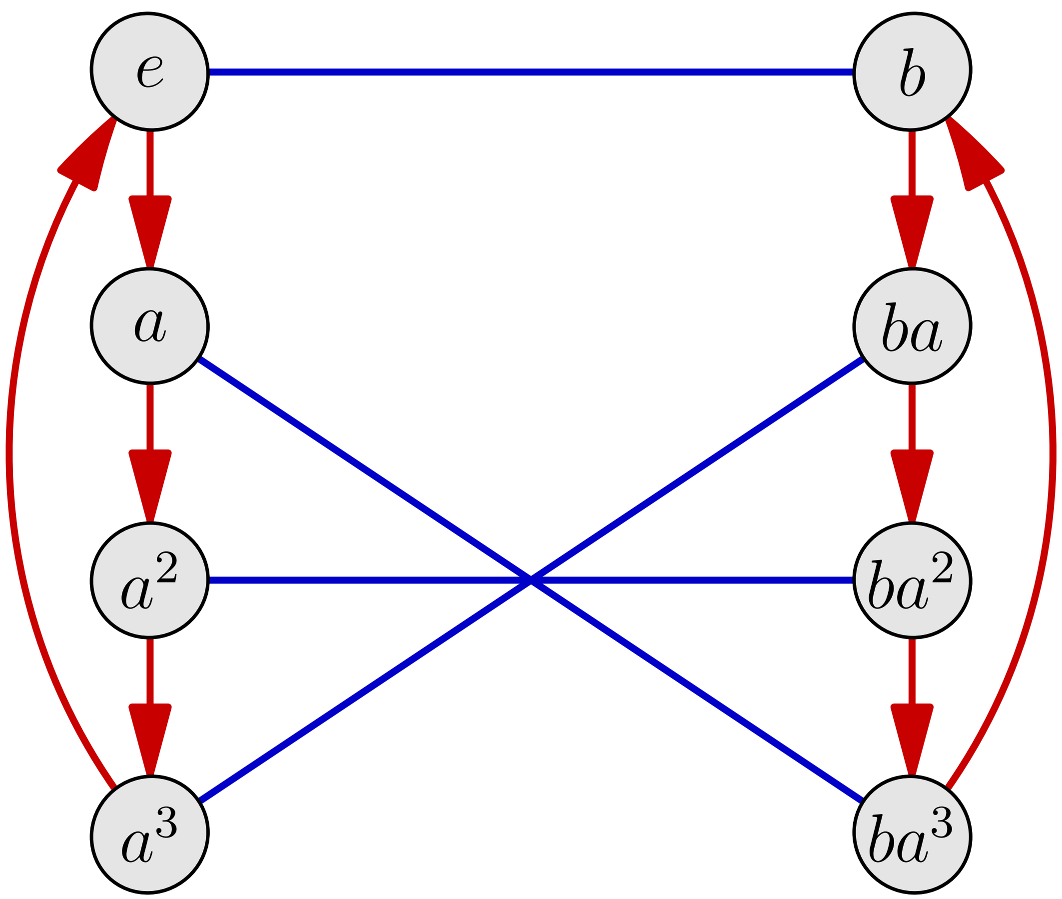
Classifying the groups of order 8

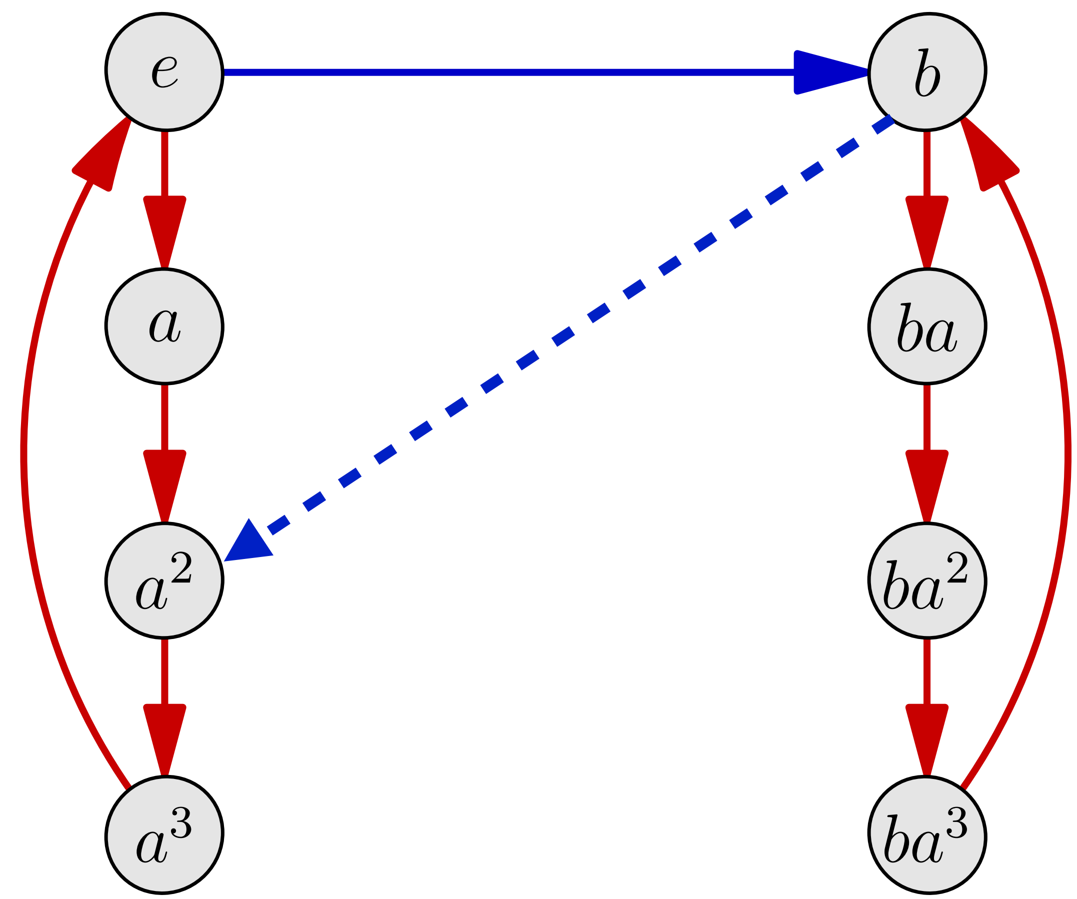




Using Sylow Theory

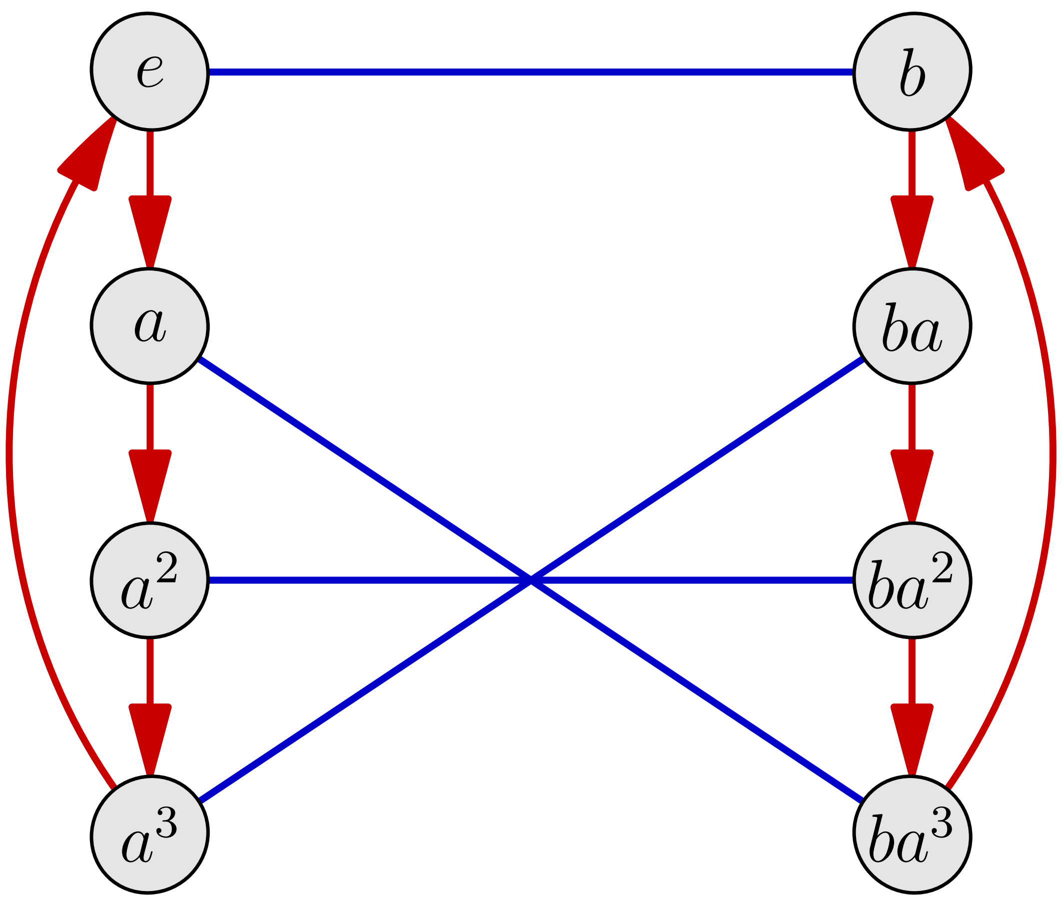
Classifying the groups of order 8

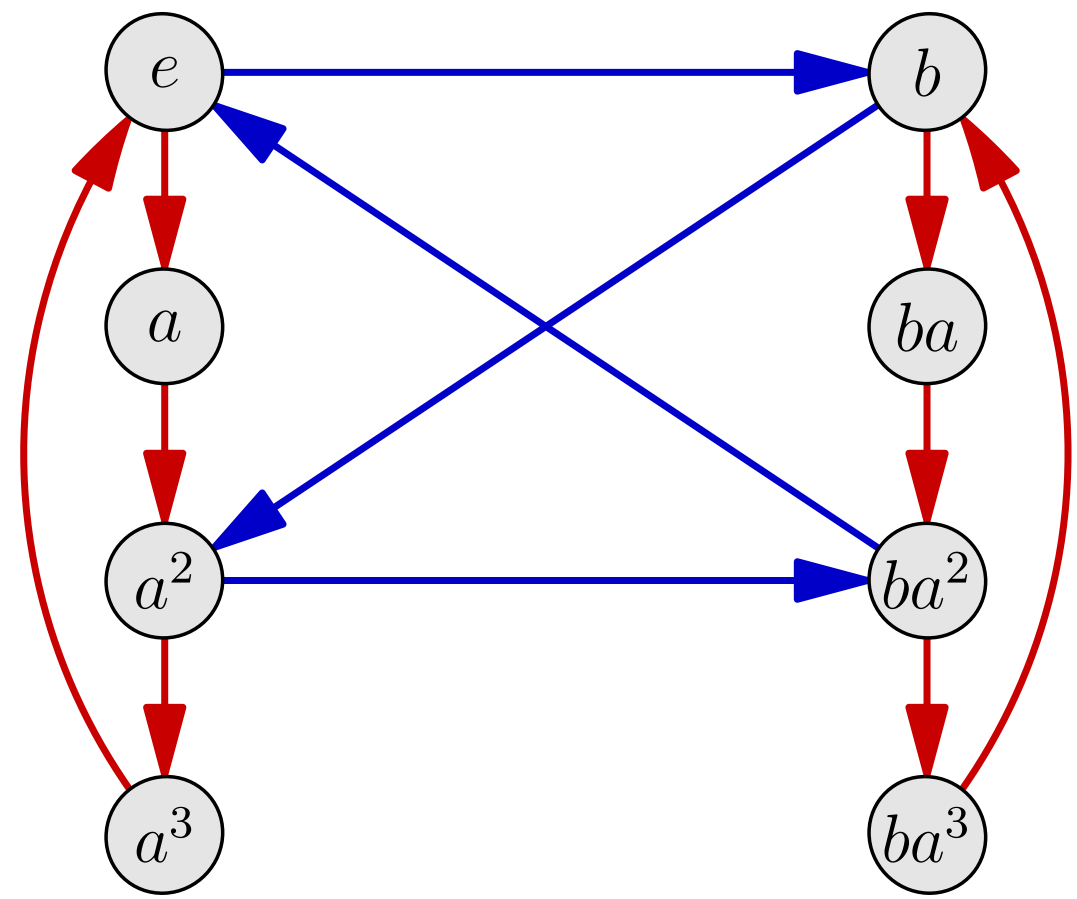




Using Sylow Theory

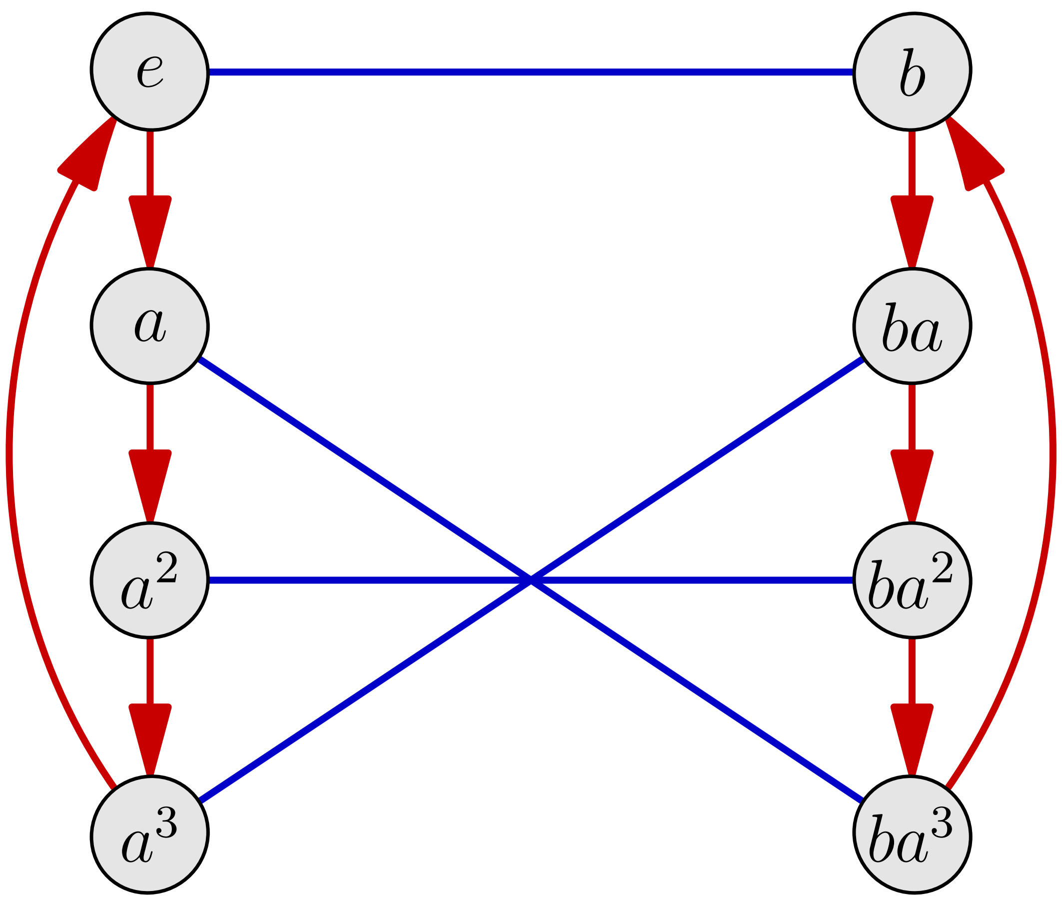
Classifying the groups of order 8

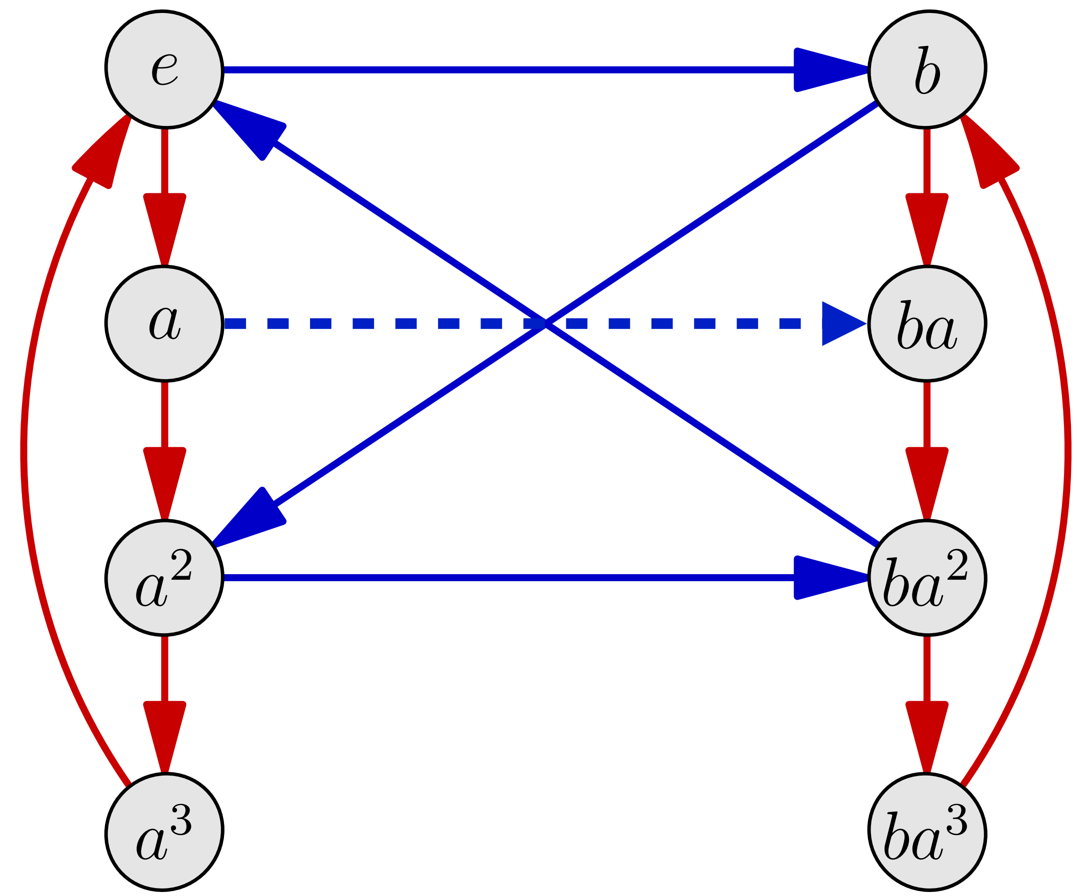




Using Sylow Theory

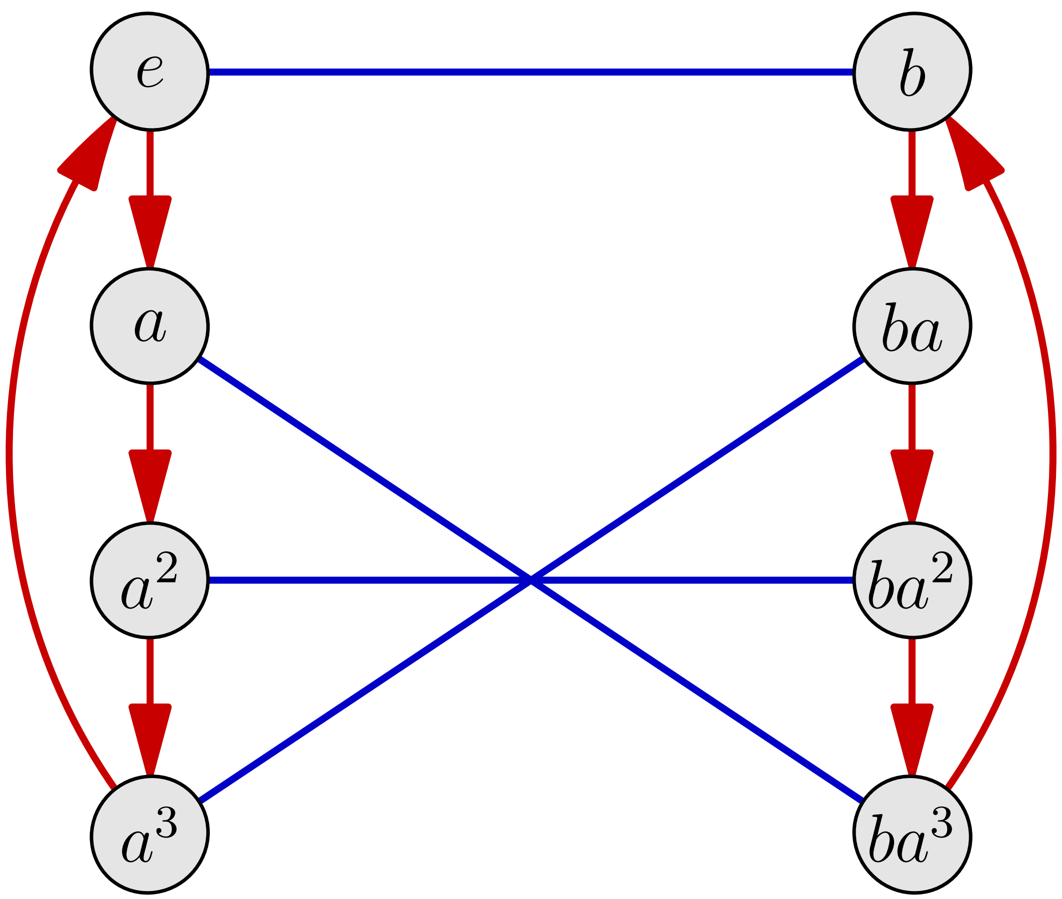
Classifying the groups of order 8

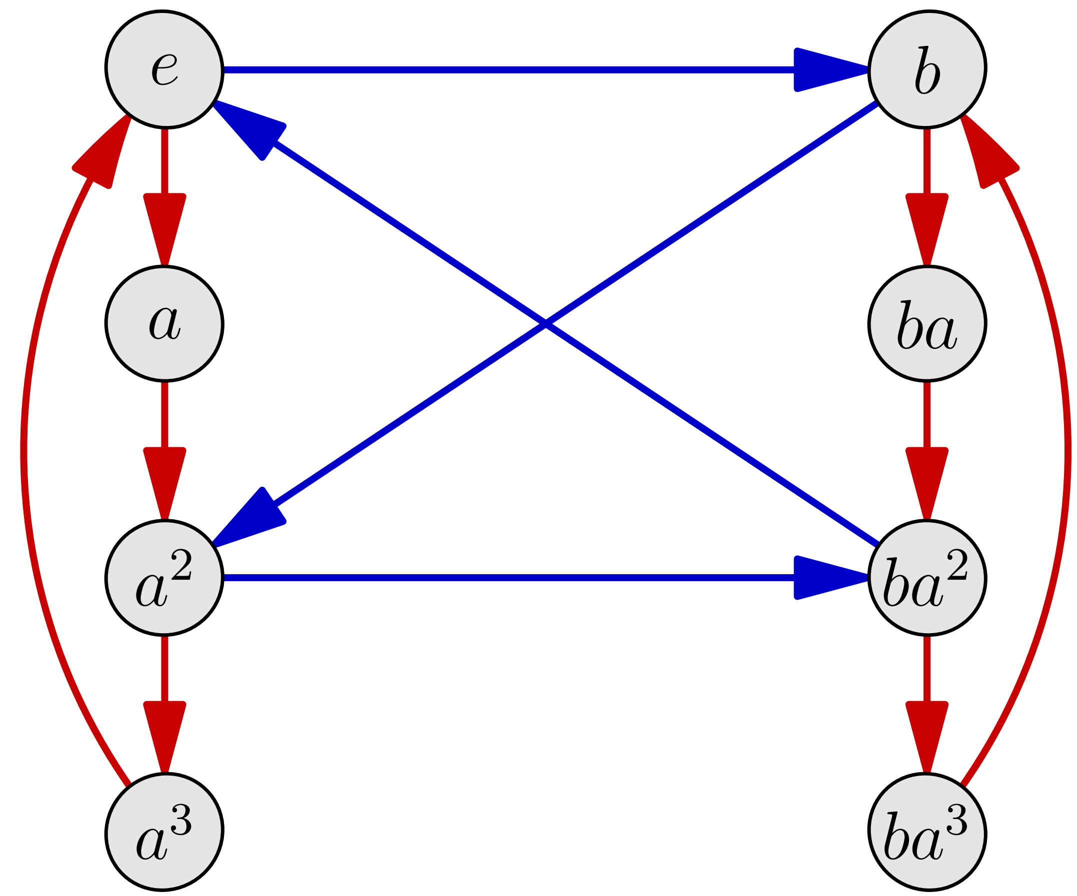




Using Sylow Theory

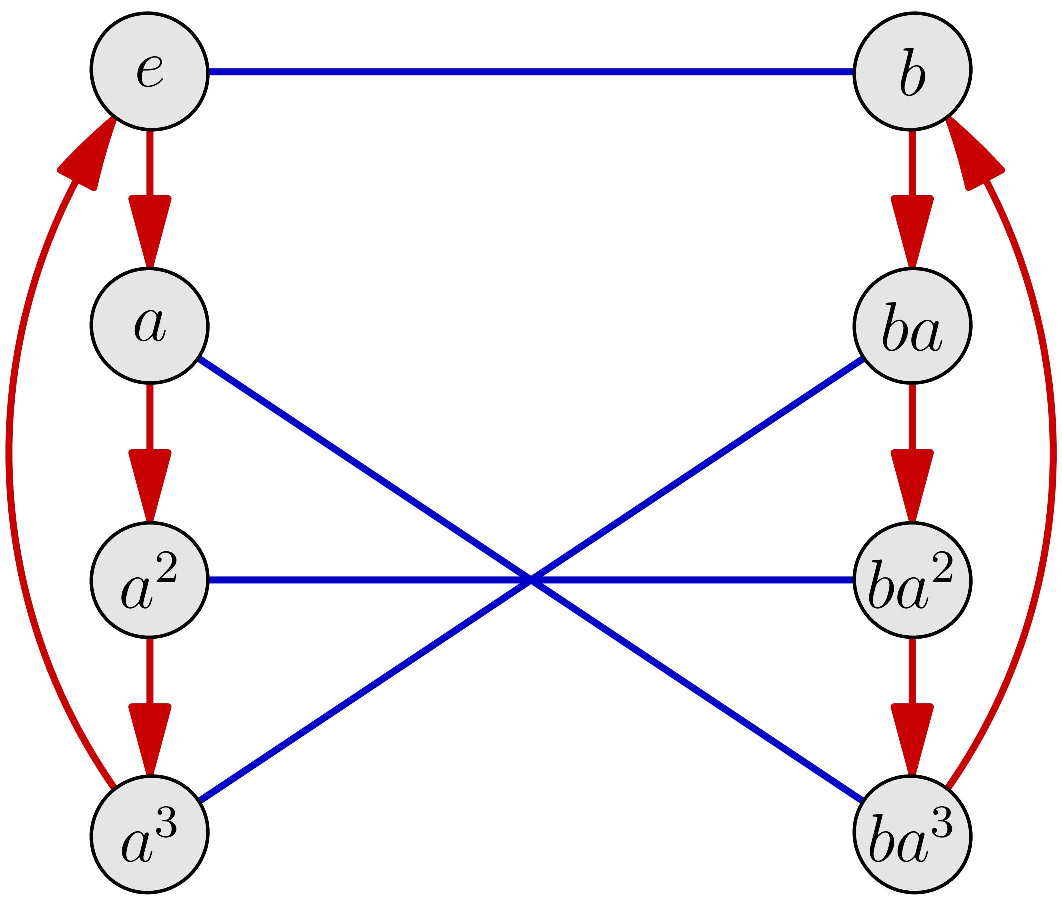
Classifying the groups of order 8

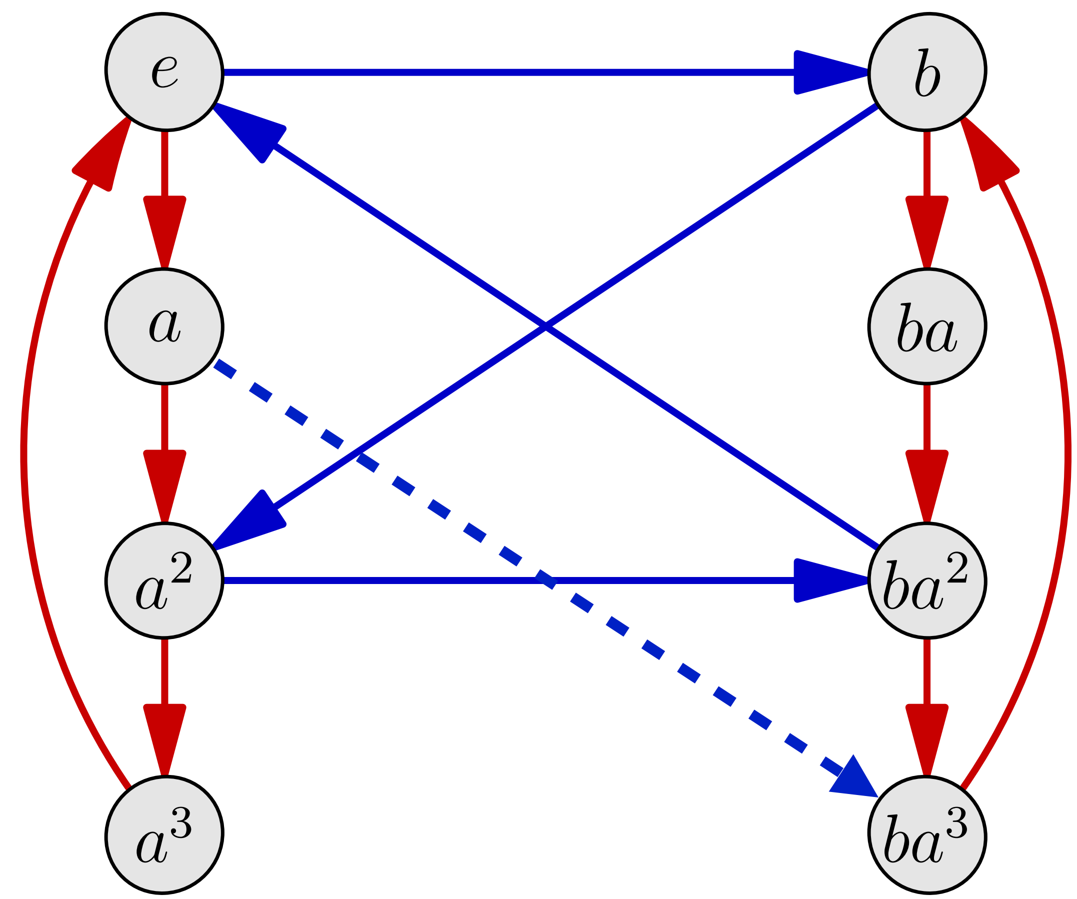




Using Sylow Theory

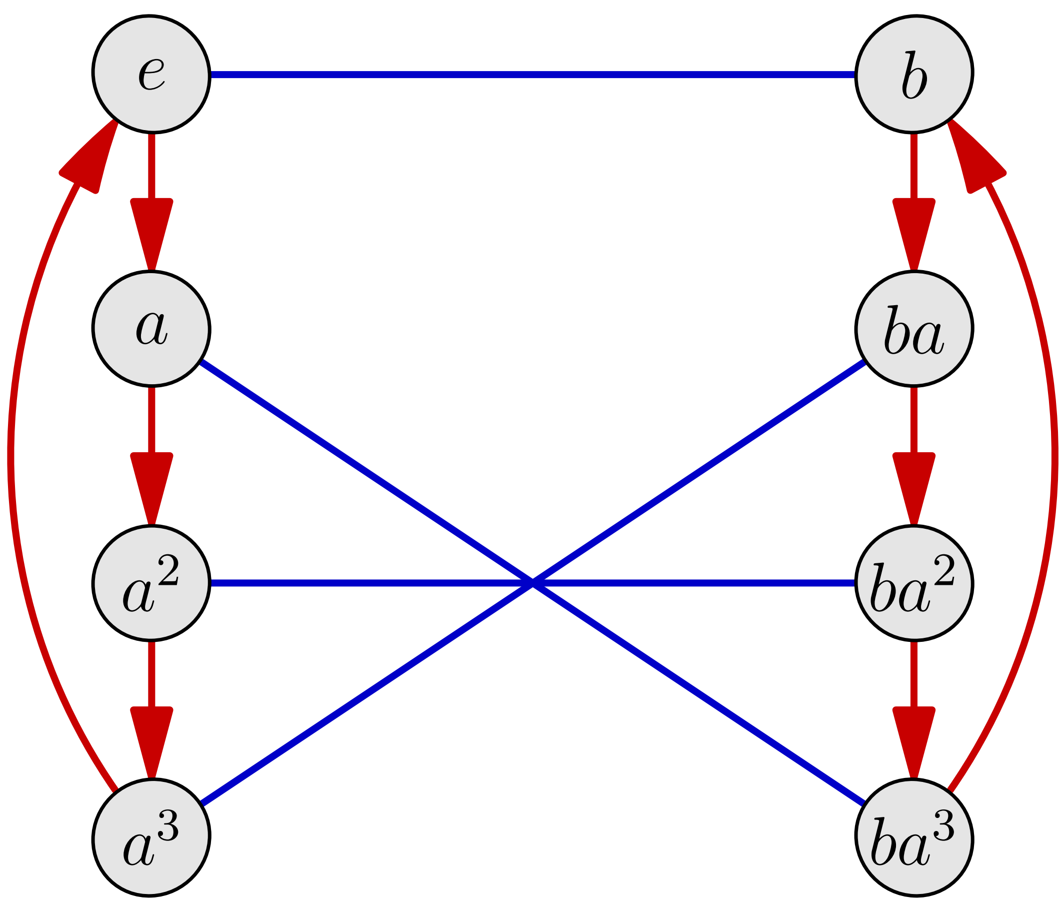
Classifying the groups of order 8



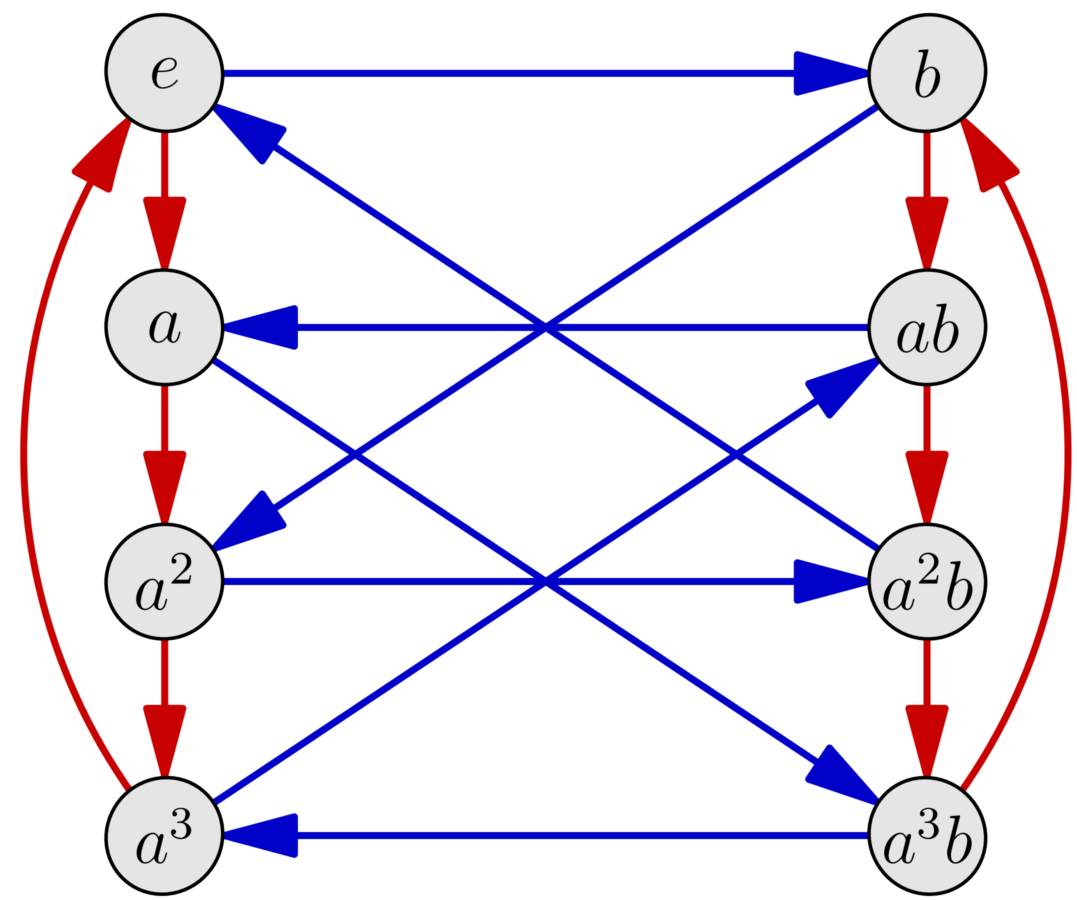


Using Sylow Theory

Classifying the groups of order 8

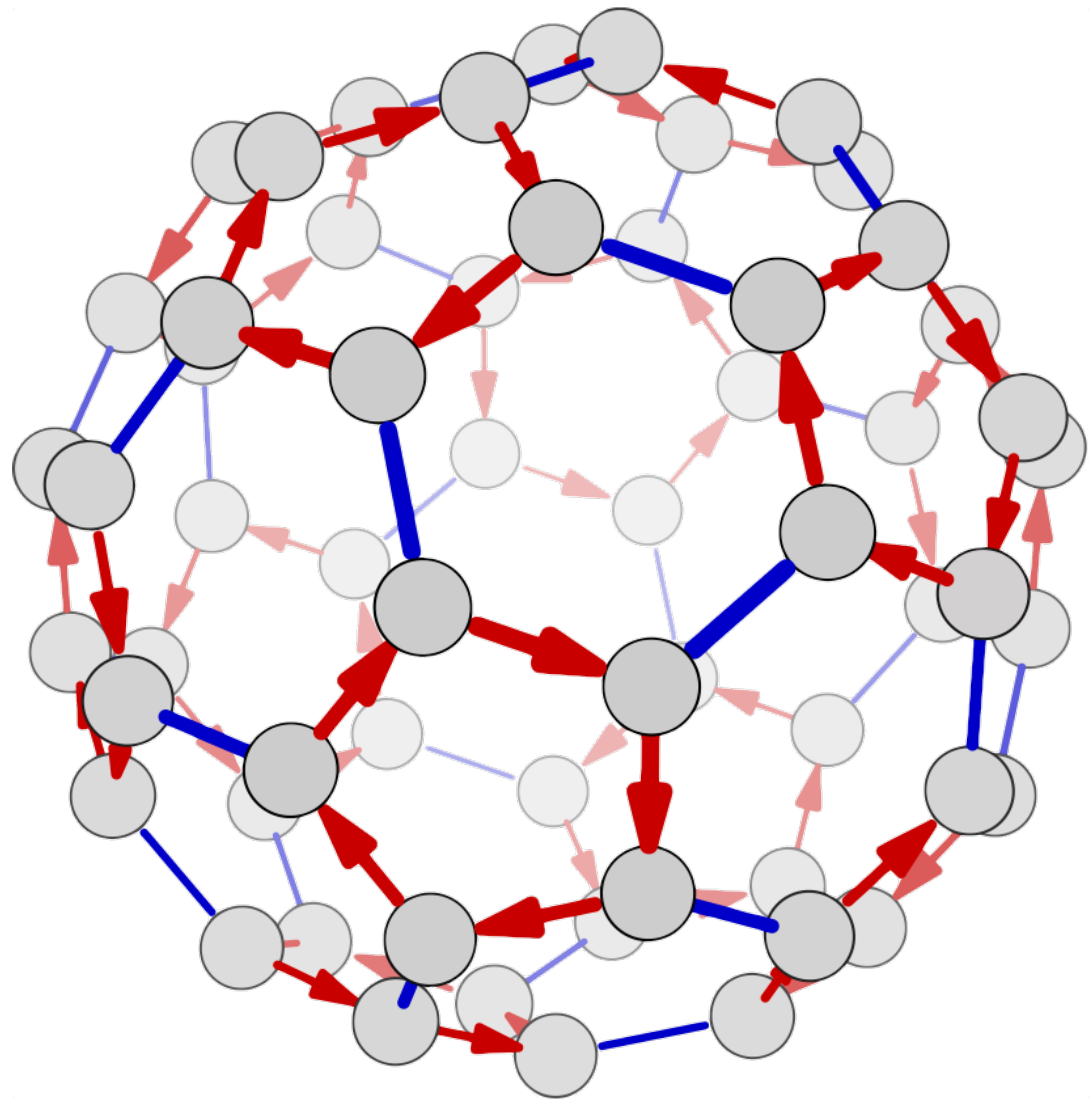


D_4



Q_4

The Surprising Pedagogical Value and Versatility of Cayley Graphs



Nathan Carter, Bentley University

nathancarter.github.io