Visual Algebra

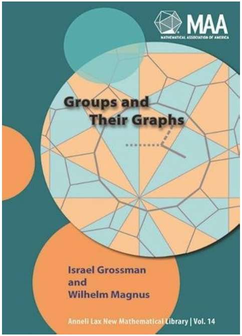
Lecture 0.2: Highlights of Visual Algebra

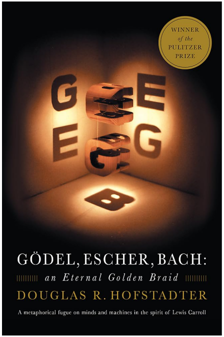
Dr. Matthew Macauley

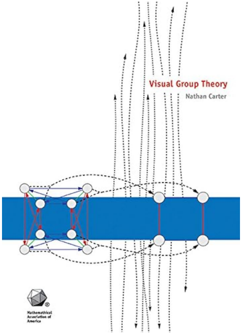
School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

A brief (incomplete) history of Visual Algebra

- **1964** Grossman and Magnus publish *Groups and Their Graphs*.
- **2002** Douglas Hofstadter teaches *Visual Group Theory & Galois Theory* at Indiana.
- **2009** Nathan Carter publishes *Visual Group Theory* (VGT). I meet him at MathFest.
- **2010** I first teach Modern Algebra at Clemson using VGT.
- **2016** I record 43 lectures on VGT.
- **2016** Dana Ernst writes *An Inquiry-Based Approach to Abstract Algebra*.
- **2019** I start writing *Visual Algebra*.
- **2024** I start re-recording a new Visual Algebra YouTube series.







Visual Group Theory vs. Visual Algebra YouTube playlists

Visual Group Theory (2016)

- 43 lectures
- 1 semester undergraduate algebra, following Nathan Carter's book (supplemented)

Visual Algebra (2025)

- $\approx$ 100 lectures
- 2+ semesters of undergraduate algebra, following my *Visual Algebra* book
- Or. . . 1+ semester of graduate algebra. (Abridged version of Ch 1–4, coming soon!)

A list of terms original to my book and video series

- A "group switchboard"
- Blue vs. red cosets
- Shoebox diagrams
- Pizza diagrams
- Semiabelian group
- Diquaternion group
- Moderately and fully unnormal
- Moderately and fully uncentral
- G-set posets
- Maximal central ascents & descents
- Chutes and ladders diagram
- The crooked ladder theorem
- (Annotated) subring lattices
- Ideal class group lattices

Visual Algebra topical outline

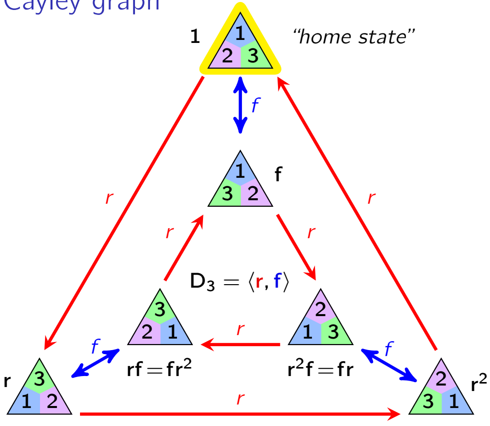
Table of contents

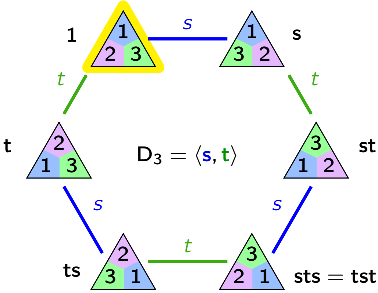
Visual Algebra courses that I teach

- **Undergraduate Algebra 1**: Chapters 1–5, half of Chapter 8.
- **Undergraduate Algebra 2**: Chapters 8–9, Chapters 6–7, Parts of Chapters 10–11.
- **Graduate Algebra 1**: Chapters 1–9.

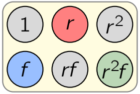
A Cayley graph

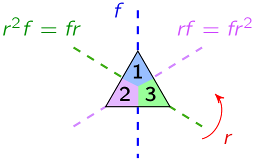
(Chapter 1)



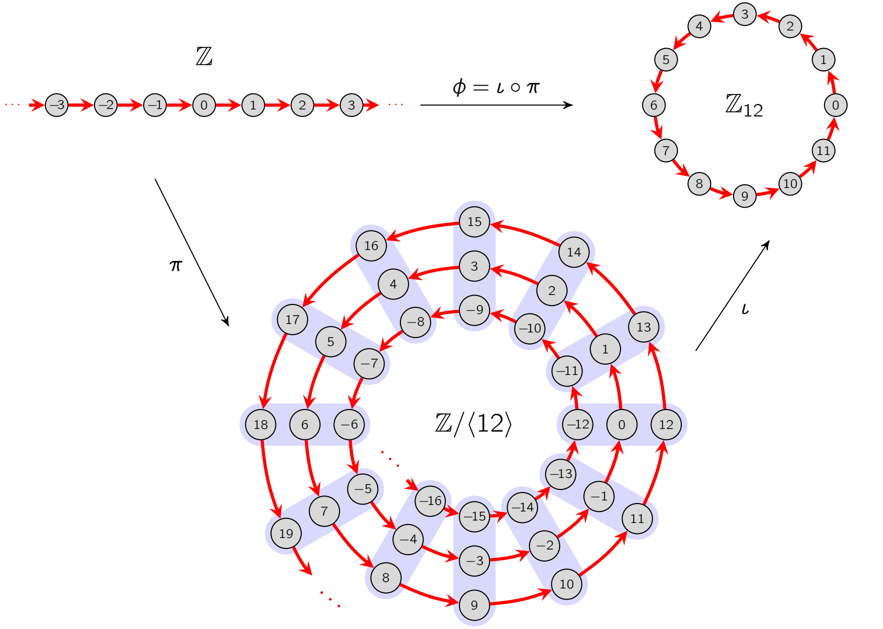


"Group switchboard"



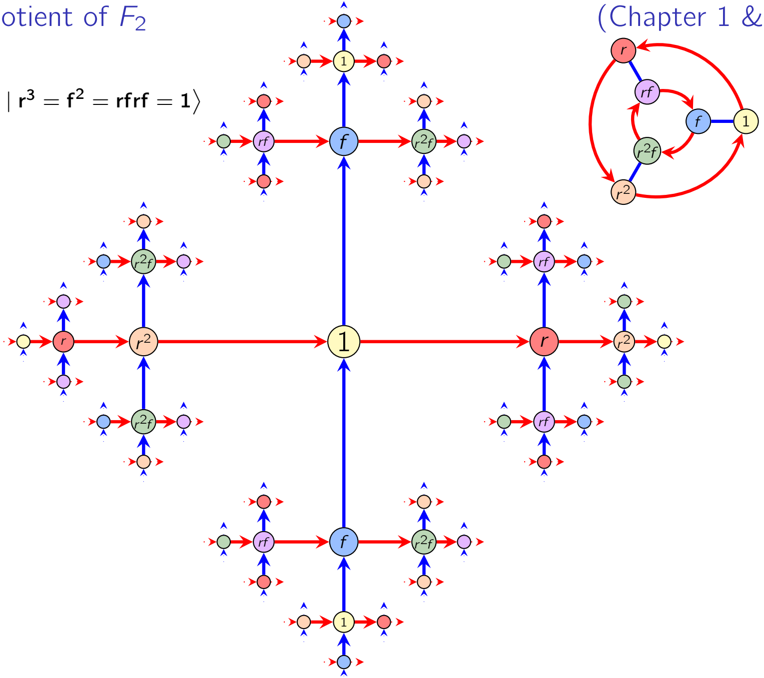


Constructing $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$ from a free group (Chapter 4)

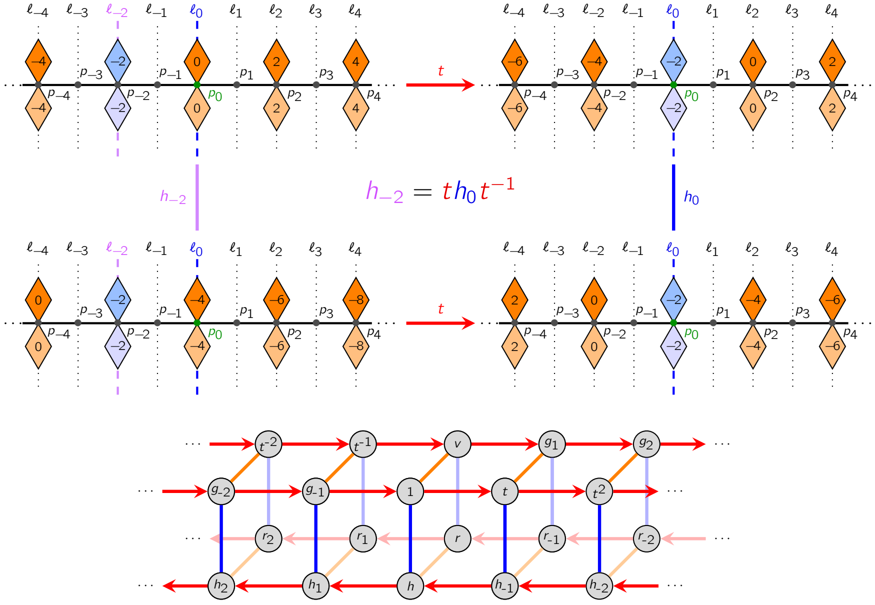


D_3 as a quotient of F_2 (Chapter 1 & 7

$\mathbf{D_3} = \langle \mathbf{r}, \mathbf{f} \mid \mathbf{r}^3 = \mathbf{f}^2 = \mathbf{rfrf} = \mathbf{1} \rangle$



Conjugation preserves structure

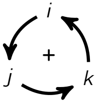


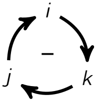
Seeing a quotient of a group (Chapter 1–4)

The quaternion group is

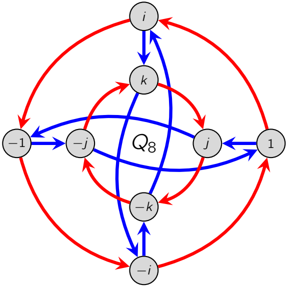
$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle \cong \left\langle \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\rangle .$$

multiplying in this direction yields a positive result

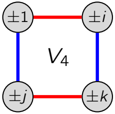




multiplying in this direction yields a negative result



	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

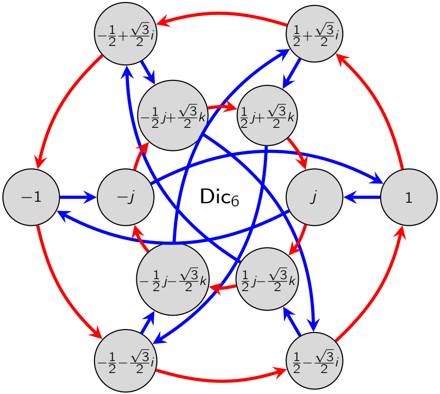


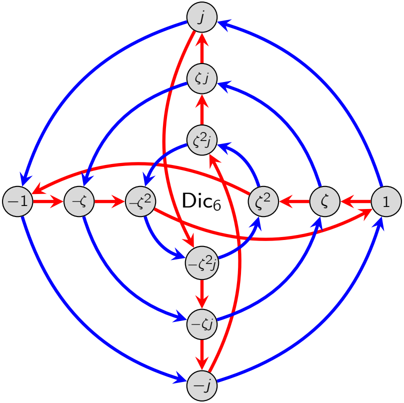
	± 1	$\pm i$	$\pm j$	$\pm k$
± 1	± 1	$\pm i$	$\pm j$	$\pm k$
$\pm i$	$\pm i$	± 1	$\pm k$	$\pm j$
$\pm j$	$\pm j$	$\pm k$	± 1	$\pm i$
$\pm k$	$\pm k$	$\pm j$	$\pm i$	± 1

The dicyclic group (Chapter 2)

Have you ever wanted to replace $i = \zeta_4 = e^{2\pi i/4}$ in Q_8 with $\zeta_n = e^{2\pi i/n}$?

$$\mathrm{Dic}_n = \langle \zeta_n, j \rangle \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\rangle .$$





The diquaternion group

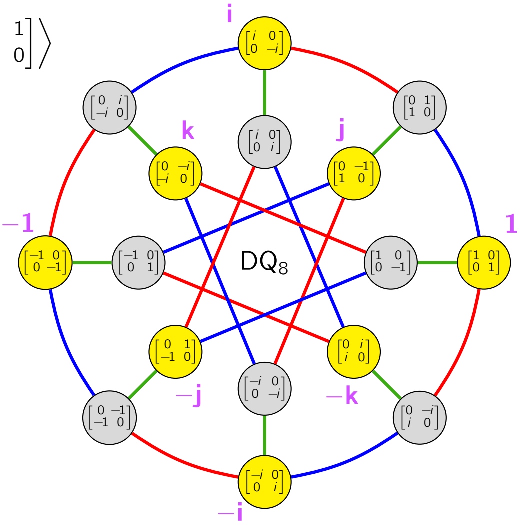
Have you ever wanted to "add a reflection" to Q_8?

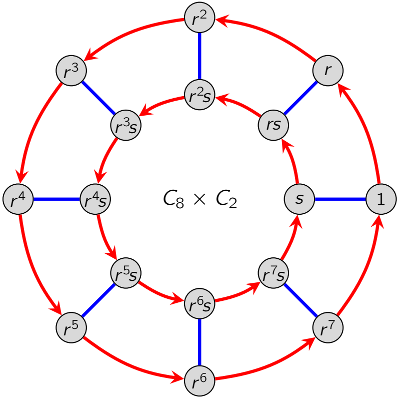
$$\mathrm{DQ}_8 = \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$$

$$X = F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

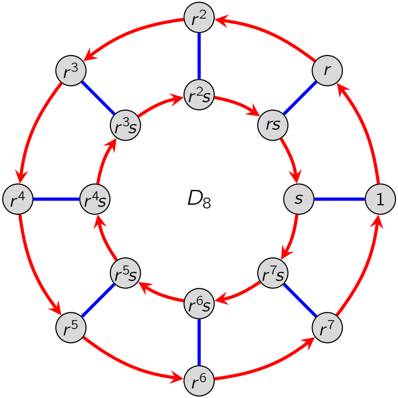
$$Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



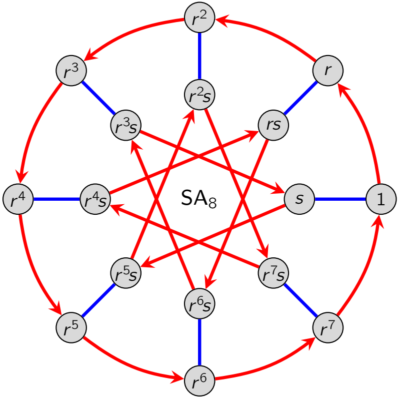


abelian

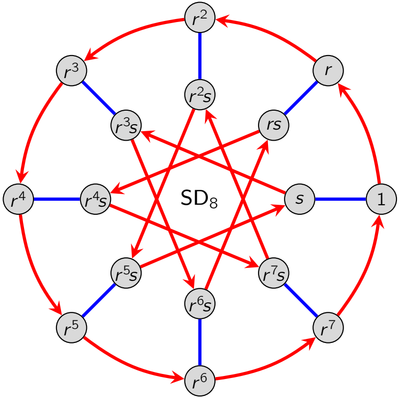


dihedral

Two relatively unknown groups (Chapter 2)

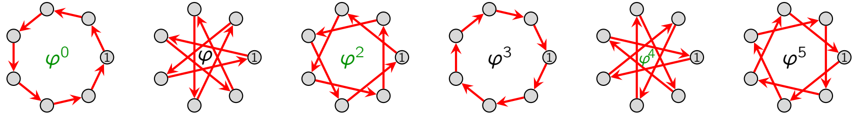


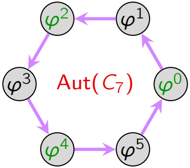
semiabelian



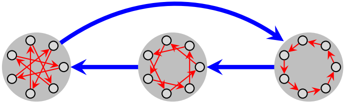
semidihedral

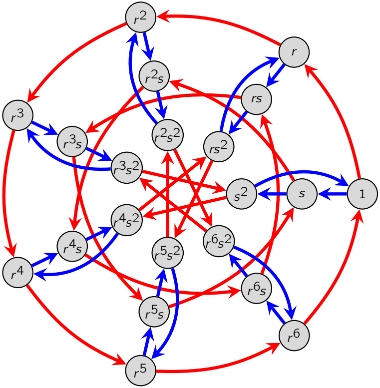
The construction of the semidirect product $C_7 \rtimes_\theta C_3$ (Chapter 2 & 4)

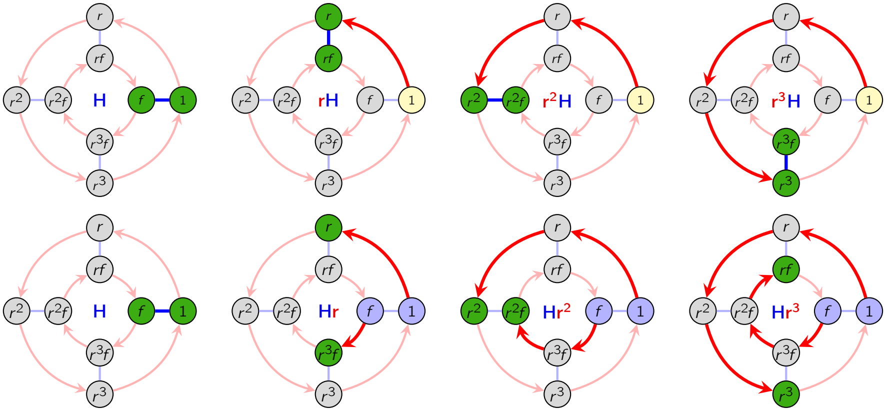




$$C_3 \xrightarrow{\theta} \mathrm{Aut}(C_7)$$
$$s^k \longmapsto \varphi^{2k}$$



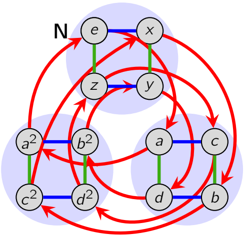


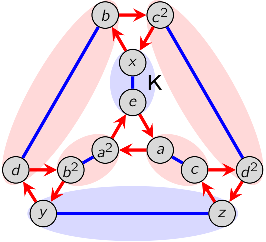


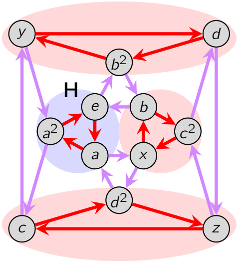
H	r^2H	rH	r^3H
f	$r^2 f$	rf	r^3
1	r^2	r	$r^3 f$

H	Hr^2			
f	fr^2	fr^3	r^3	Hr^3
1	r^2	r	fr	Hr

The normalizer is the "union of blue cosets."







(124)	(234)	(143)	(132)
(123)	(243)	(142)	(134)
e	(12)(34)	(13)(24)	(14)(23)

"*normal*"

(124)	(234)	(143)	(132)
(123)	(243)	(142)	(134)
e	(12)(34)	(13)(24)	(14)(23)

"*moderately unnormal*"

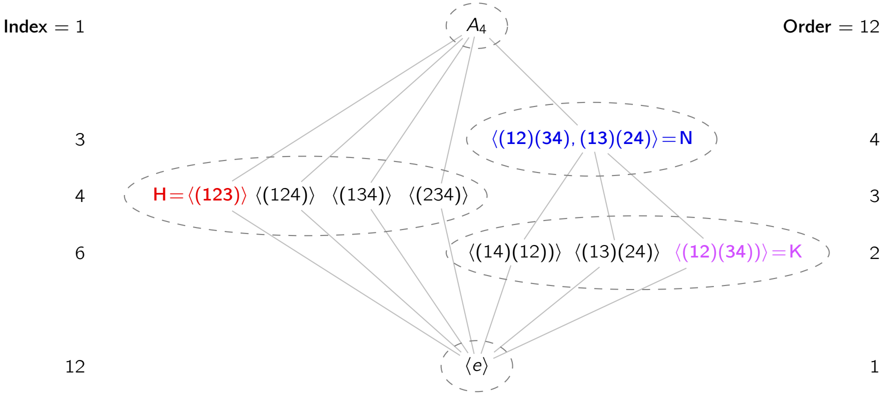
(14)(23)	(142)	(143)
(13)(24)	(243)	(124)
(12)(34)	(134)	(234)
e	(123)	(132)

"*fully unnormal*"

Key idea

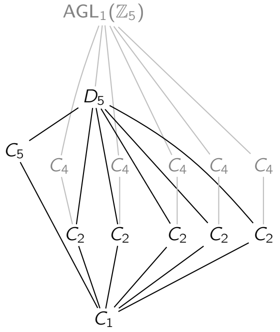
Two measures of normality are:

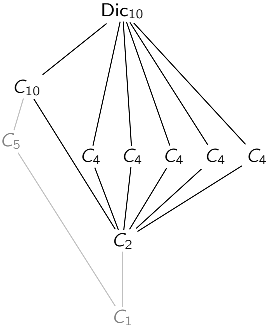
- The proportion of cosets that are blue.
- The width of a "conjugate fan"



Subgroups vs. quotients (Chapter 4)

The difference between subgroups and quotient maps can be seen in the subgroup lattice!

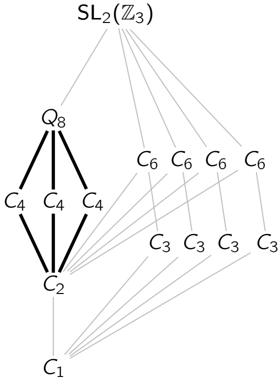


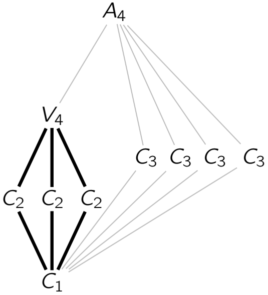


Subgroups, quotients, and subquotients (Chapter 4)

Often, we'll see familiar subgroup lattices in the middle of a larger lattice.

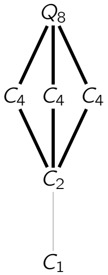
These are called **subquotients**.





subgroup of a quotient

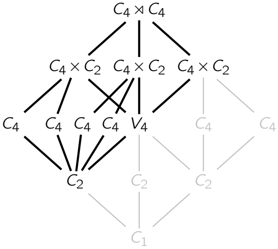
quotient of a subgroup



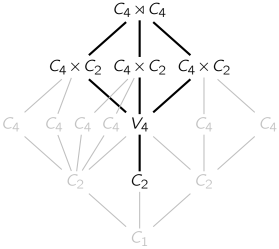
Big idea

We can deduce the structure of G/N from G, and vice-versa

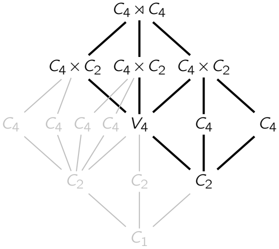
Fun exercise: Find the conjugacy classes of $C_4 \rtimes C_4$ by inspection alone.



Quotient $\cong D_4$

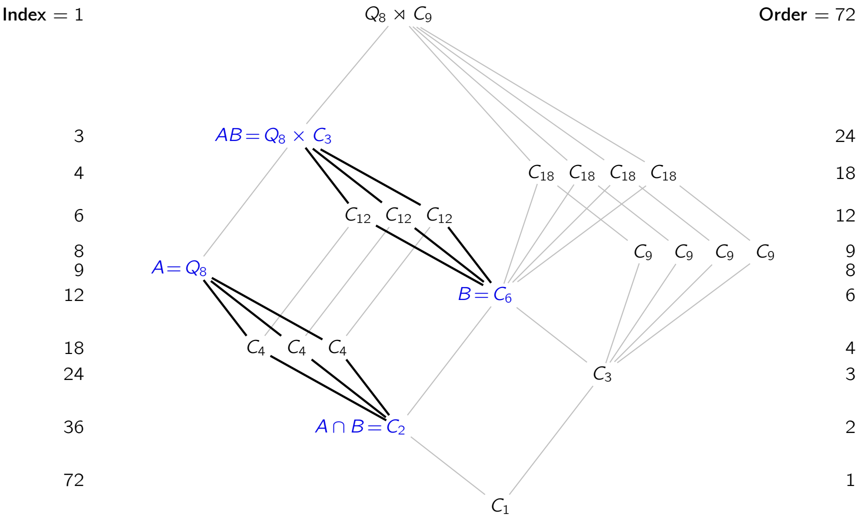


Quotient $\cong Q_8$

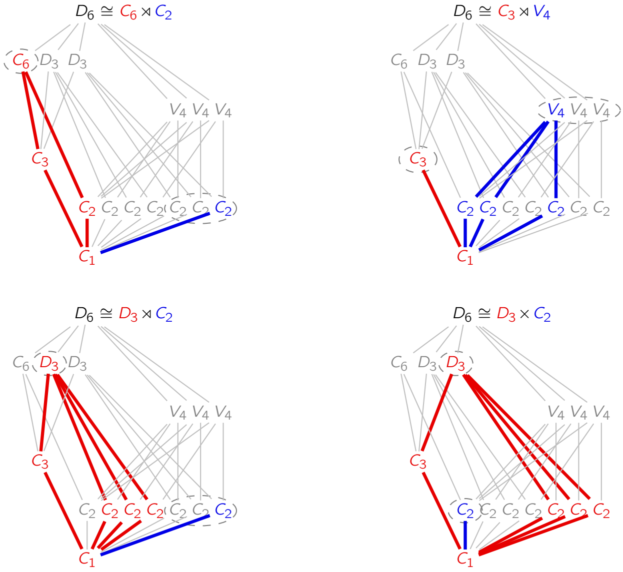


Quotient $\cong C_4 \times C_2$

The diamond theorem: duality of subquotients (Chapter 4)

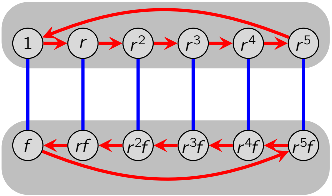


Decompositions of D_6 into direct and semdirect products (Chapter 4)

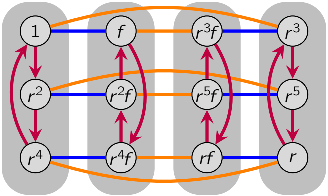


Decompositions of D_6 into direct and semidirect products (Chapter 4)

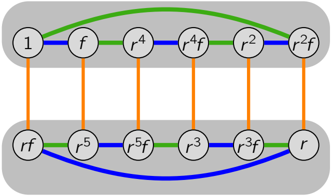
$C_6 \rtimes C_2$



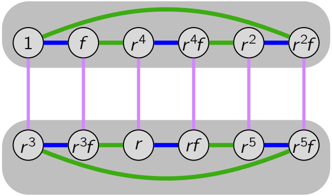
$C_3 \rtimes V_4$



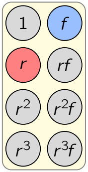
$D_3 \rtimes C_2$

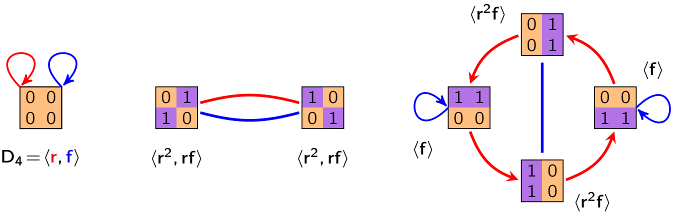


$D_3 \times C_2$

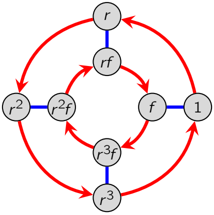


"Group switchboard"

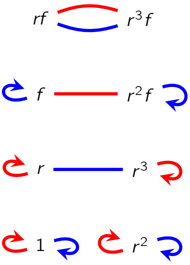




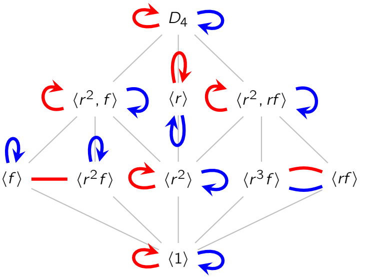
We say that: "$G = D_4$ *acts on…*"



"… itself by right-multiplication"

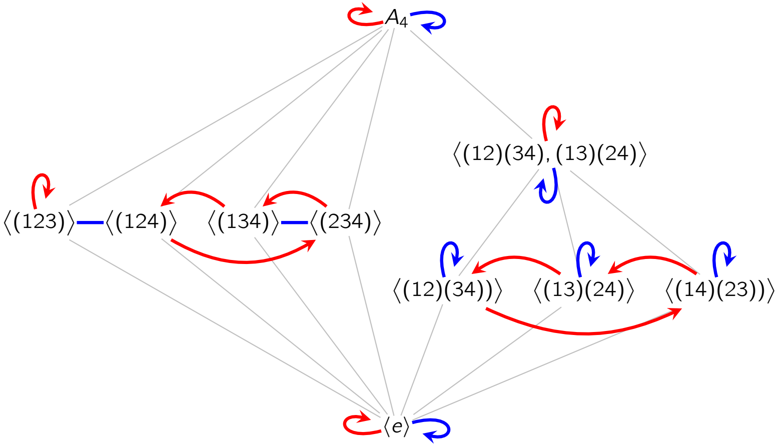


"… itself by conjugation"

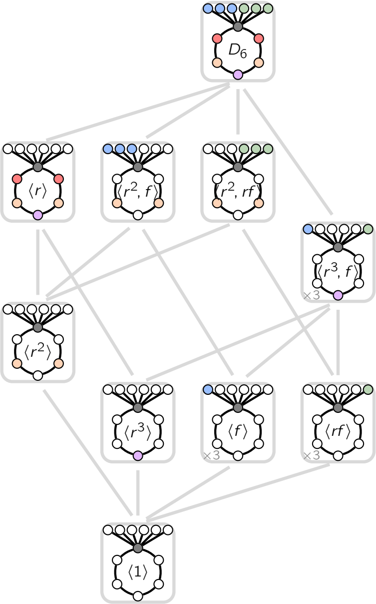


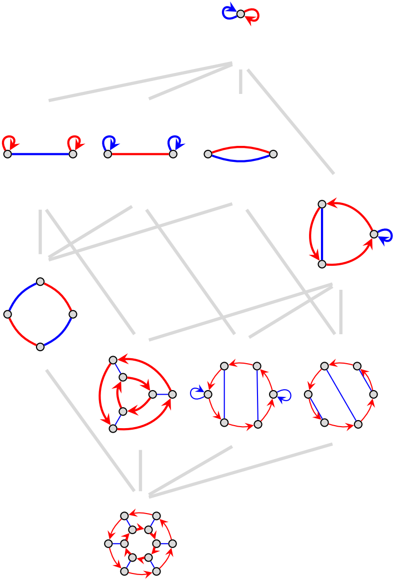
"… its subgroups by conjugation"

Here is an example of $G = A_4 = \langle (123), (12)(34) \rangle$ acting on its subgroups.

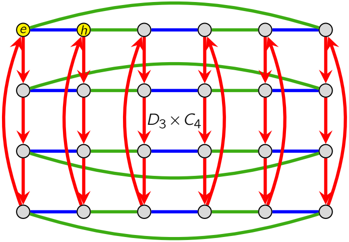


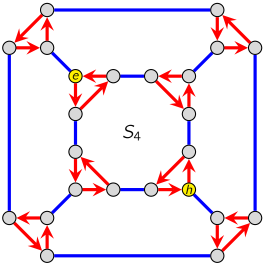
Collapsing a Cayley graph by right cosets (Chapter 5)

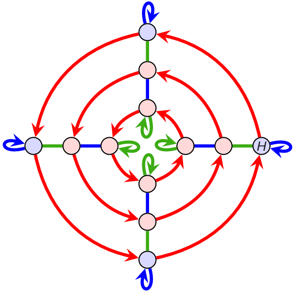


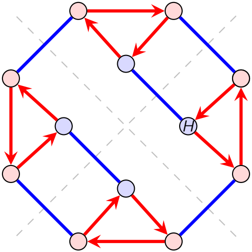


Two examples of transitive G-sets (Chapter 5)







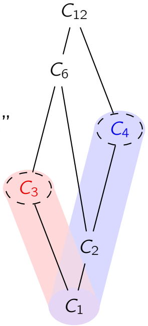


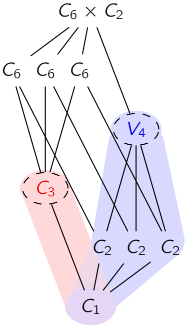
The five groups of order 12

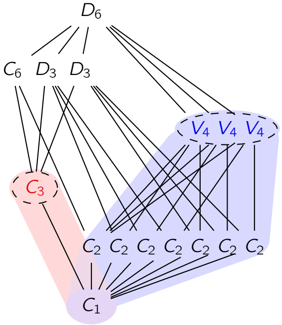
Sylow p-subgroups come in "towers."

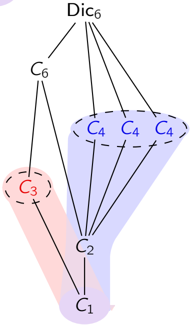
Sylow 2-subgroups are blue

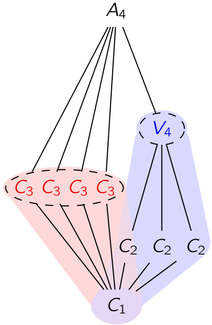
Sylow 3-subgroups are red.



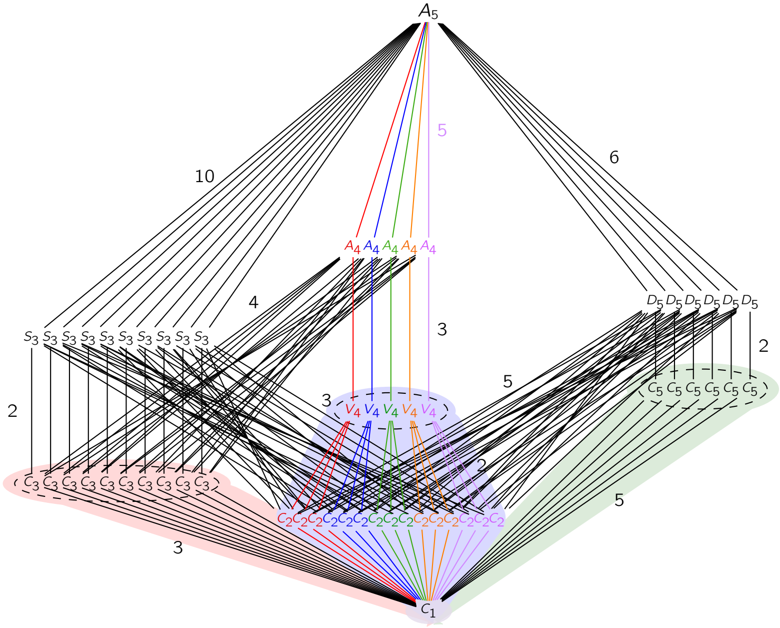




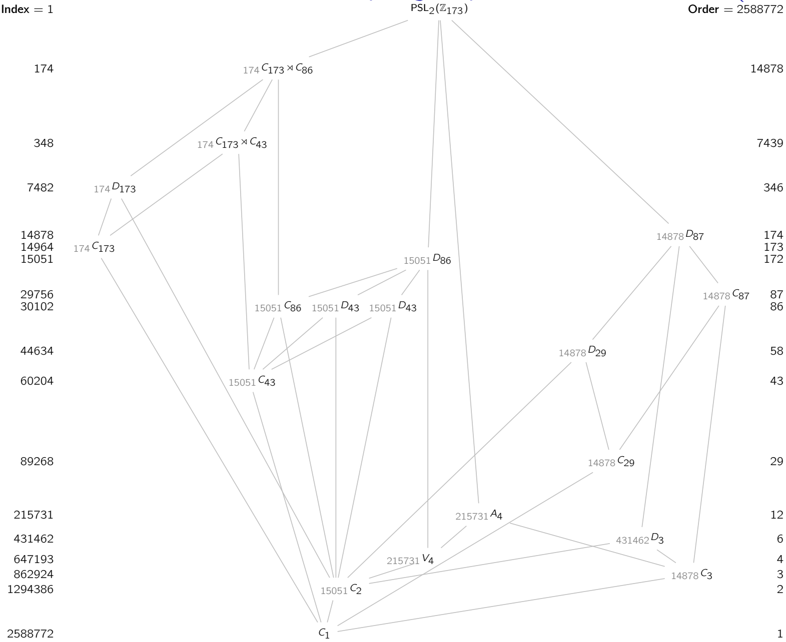




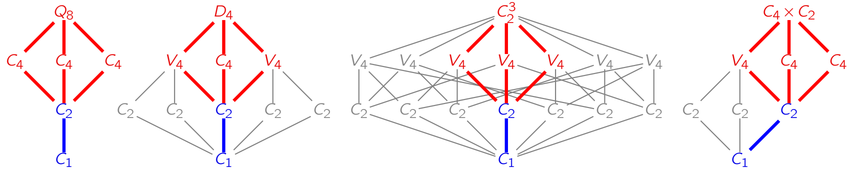
The smallest nonabelian simple group (Chapter 5)



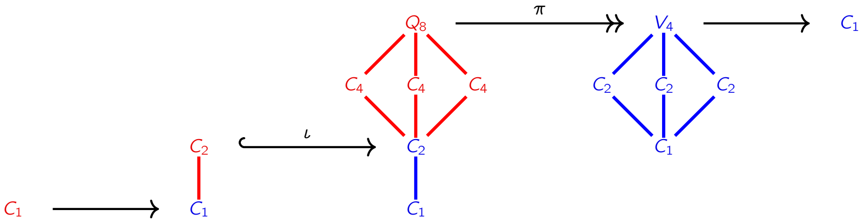
The 71[st] smallest nonabelian simple group (Chapter 6)



Here are four **extensions** of the group V_4 by C_2.



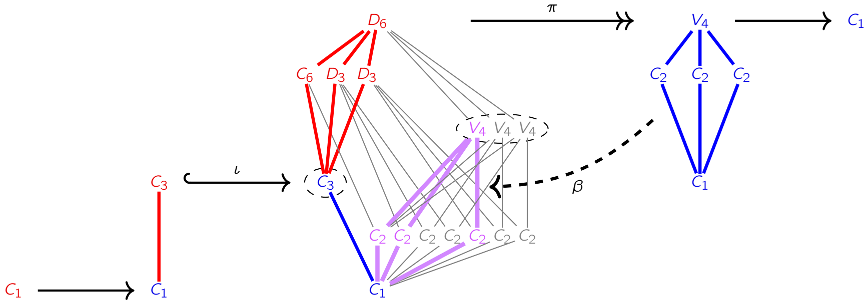
Each can be encoded by a **short exact sequence**.



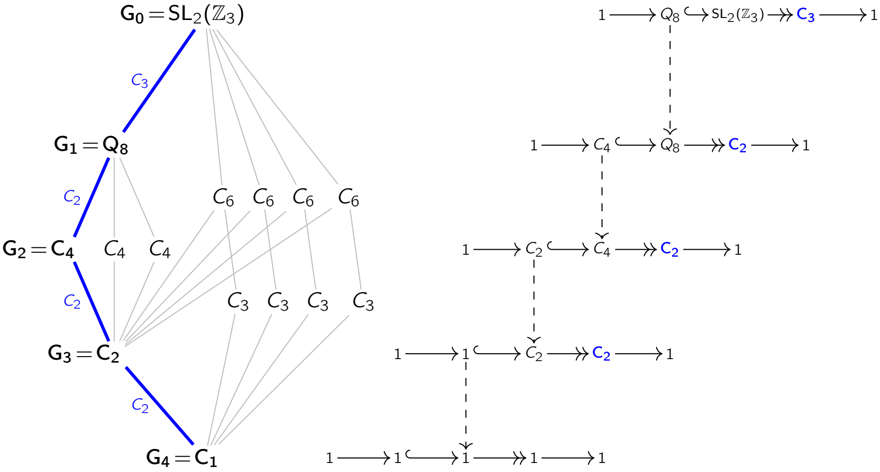
Definition

A short exact sequence **splits** if there is a backwards map $\beta \colon H \to G$ for which $\pi \circ \beta = \mathrm{Id}_H$:

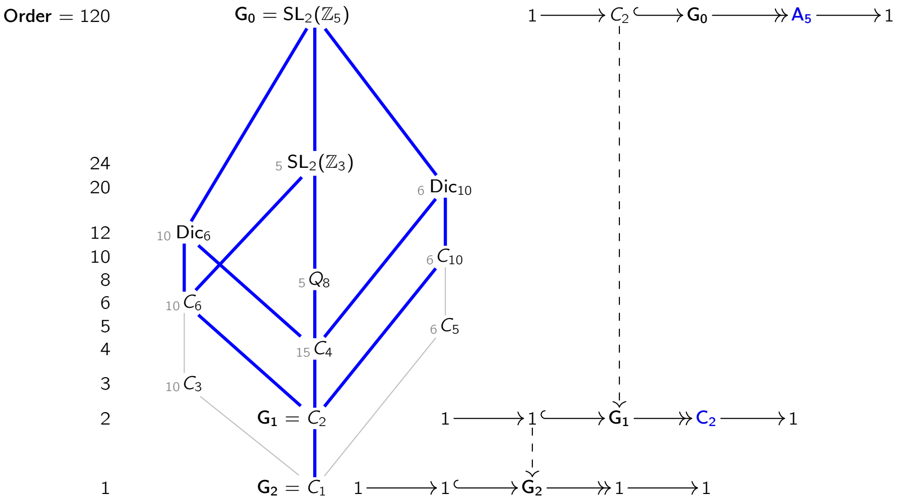
$$1 \longrightarrow N \xrightarrow{\ \iota\ } G \underset{\beta}{\overset{\pi}{\rightleftarrows}} H \longrightarrow 1$$

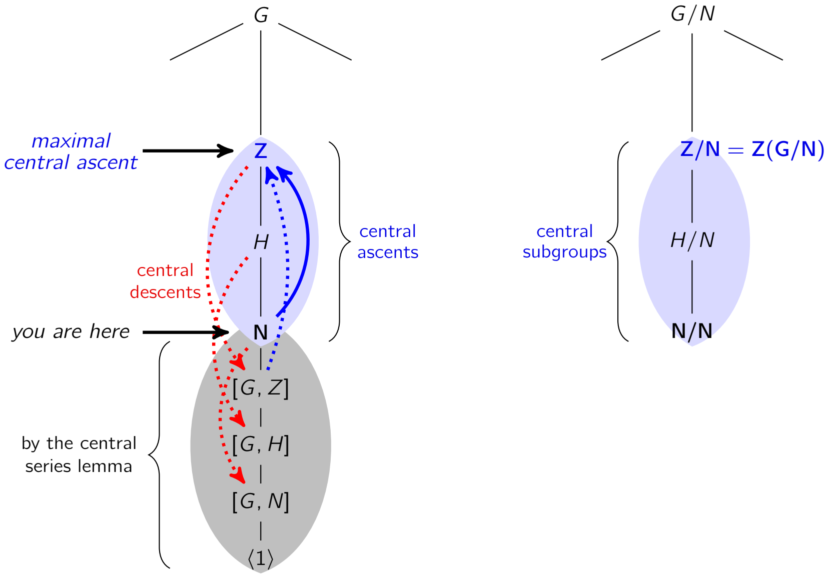


Composition series of a solvable group

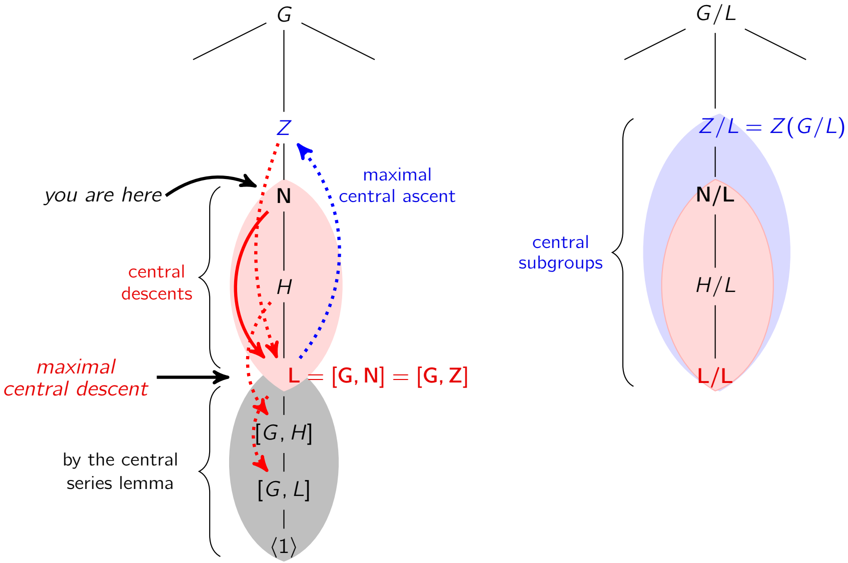


Composition series of a non-solvable group (Chapter 6)



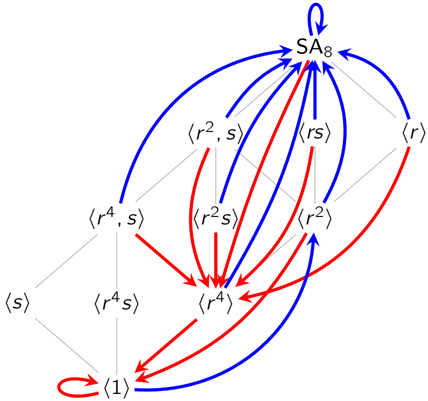

G
maximal
central ascent
Z
H
central
descents
you are here
N
[G, Z]
[G, H]
[G, N]
⟨1⟩
central
ascents
by the central
series lemma
G/N
Z/N = Z(G/N)
central
subgroups
H/N
N/N

Central descents (Chapter 6)



From each $N \trianglelefteq G$ is a

- maximal central descent $N \searrow L$, where $L = [G, N]$,
- maximal central ascent $N \nearrow Z$, where $Z/N = Z(G/N)$.



The ascending and descending central series can be read right off this diagram!

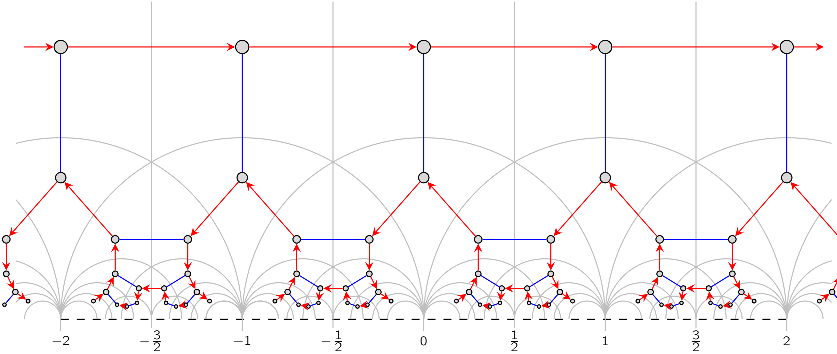
A simply transitive action of $\mathrm{PSL}_2(\mathbb{Z})$ (Chapter 5, 7)

The projective special linear group

$$\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\langle -I \rangle, \qquad \text{where } \mathrm{SL}_2(\mathbb{Z}) = \Bigg\langle \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{S}, \underbrace{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}}_{T} \Bigg\rangle$$

defines a tiling of hyperbolic ideal triangles in the upper half-plane via

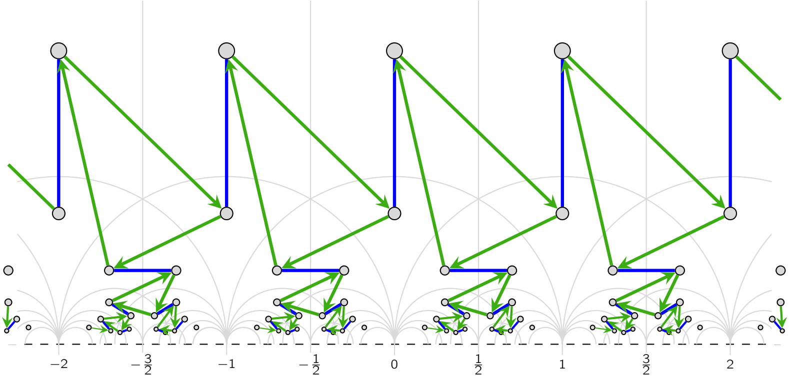
$$S\colon z \longmapsto \frac{0z-1}{z+0} = -\frac{1}{z}, \qquad \text{and} \qquad T\colon z \longmapsto \frac{z+1}{0z+1} = z+1,$$



$\mathrm{PSL}_2(\mathbb{Z}) \cong C_3 * C_2$

$\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \mid S^2 = (ST)^6 = I \rangle$, $\quad S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $\quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\quad ST = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$,

Then $\mathrm{PSL}_2(\mathbb{Z}) \cong \langle A, B \rangle$, where $A = \pm ST$ and $B = \pm S$.



The four rings of order 6

The additive group $\mathbb{Z}_6$ is a ring, where multiplication is defined modulo 6.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

However, this is not the only way to add a ring structure to $(\mathbb{Z}_6, +)$.

$\times$	0	a	$2a$	$3a$	$4a$	$5a$
0	0	0	0	0	0	0
a	0	0	0	0	0	0
$2a$	0	0	0	0	0	0
$3a$	0	0	0	0	0	0
$4a$	0	0	0	0	0	0
$5a$	0	0	0	0	0	0

$\langle 6 \rangle \cong 6\mathbb{Z}_6 \subseteq \mathbb{Z}_{36}$,

$\times$	0	a	$2a$	$3a$	$4a$	$5a$
0	0	0	0	0	0	0
a	0	$4a$	$2a$	0	$4a$	$2a$
$2a$	0	$2a$	$4a$	0	$2a$	$4a$
$3a$	0	0	0	0	0	0
$4a$	0	$4a$	$2a$	0	$4a$	$2a$
$5a$	0	$2a$	$4a$	0	$2a$	$4a$

$\langle 2 \rangle \cong 2\mathbb{Z}_6 \subseteq \mathbb{Z}_{12}$,

$\times$	0	a	$2a$	$3a$	$4a$	$5a$
0	0	0	0	0	0	0
a	0	$3a$	0	$3a$	0	$3a$
$2a$	0	0	0	0	0	0
$3a$	0	$3a$	0	$3a$	0	$3a$
$4a$	0	0	0	0	0	0
$5a$	0	$3a$	0	$3a$	0	$4a$

$\langle 3 \rangle \cong 3\mathbb{Z}_6 \subseteq \mathbb{Z}_{18}$.

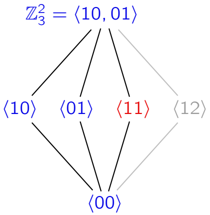
A familiar example (Chapter 8)

The subring $\langle 10 \rangle = \{00, 10, 20\}$ is an ideal of $\mathbb{Z}_3^2 = \{ab \mid a, b \in \mathbb{Z}_3\}$.

+	00	10	20	01	11	21	02	12	22
00	00	10	20	01	11	21	02	12	22
10	10	**-0**	00	11	**-1**	01	12	**-2**	02
20	20	00	10	21	01	11	22	02	12
01	01	11	21	02	12	22	00	10	20
11	11	**-1**	01	12	**-2**	02	10	**-0**	00
21	21	01	11	22	02	12	20	00	10
02	02	12	22	00	10	20	01	11	21
12	12	**-2**	02	10	**-0**	00	11	**-1**	01
22	22	02	12	20	00	10	21	01	11

×	00	10	20	01	11	21	02	12	22
00	00	00	00	00	00	00	00	00	00
10	00	**-0**	20	00	**-0**	20	00	**-0**	20
20	00	20	10	00	20	10	00	20	10
01	00	00	00	01	01	01	02	02	02
11	00	**-0**	20	01	**-1**	21	02	**-2**	22
21	00	20	10	01	21	11	02	22	12
02	00	00	00	02	02	02	01	01	01
12	00	**-0**	20	02	**-2**	22	01	**-1**	21
22	00	20	10	02	22	12	01	21	11

The three types of ring substructures (Chapter 8)

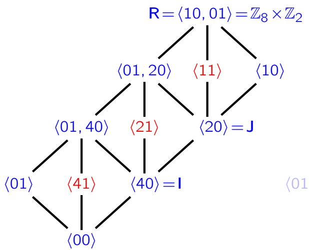


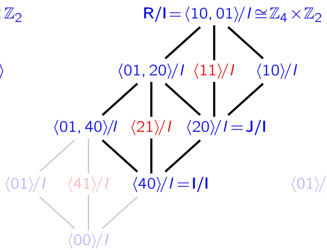
- The subgroup $\langle 10 \rangle$ is an ideal.
- The subgroup $\langle 11 \rangle$ is a subring but not an ideal.
- The subgroup $\langle 12 \rangle$ is a not even a subring.

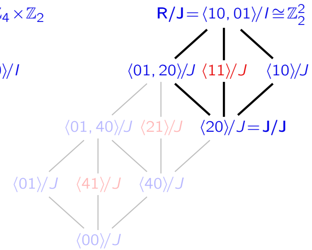
×	00	11	22	12	21	10	20	01	02
00	00	00	00	00	00	00	00	00	00
11	00	11	22	12	21	10	20	01	02
22	00	22	11	21	12	20	10	02	01
12	00	12	21	11	22	10	20	01	02
21	00	21	12	22	11	20	10	02	01
10	00	10	20	10	20	10	20	00	00
20	00	20	10	20	10	20	10	00	00
01	00	01	02	02	01	00	00	01	02
02	00	02	01	01	02	00	00	02	01

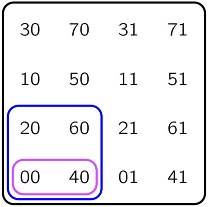
×	00	12	21	10	22	01	11	20	02
00	00	00	00	00	00	00	00	00	00
12	00	11	22	10	21	02	12	20	01
21	00	22	11	20	12	01	21	10	02
10	00	10	20	10	20	00	10	20	00
22	00	21	12	20	11	02	22	10	01
01	00	02	01	00	02	01	01	00	02
11	00	12	21	10	22	01	11	20	02
20	00	20	10	20	10	00	20	10	00
02	00	01	02	00	01	02	02	00	01

The fraction theorem: quotients of quotients (Chapter 8)

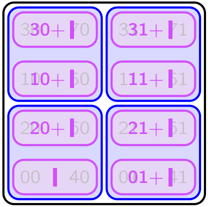






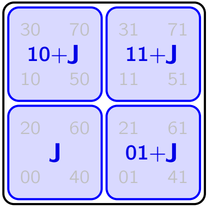


$I \leq J \leq R$



R/I consists of 8 cosets

$J/I = \{I,\ 20+I\}$

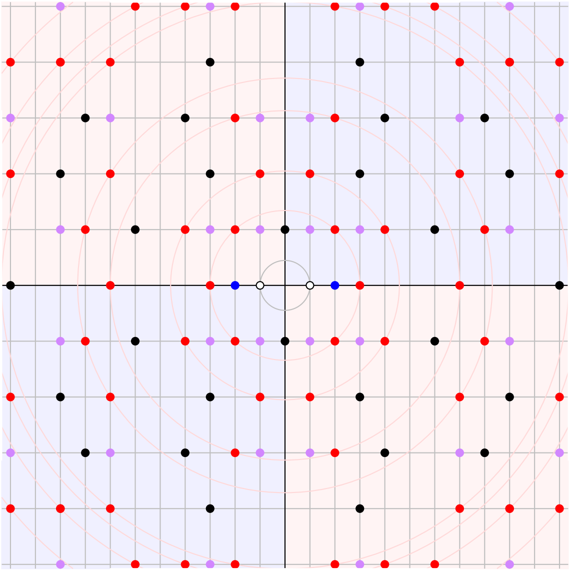


R/J consists of 4 cosets

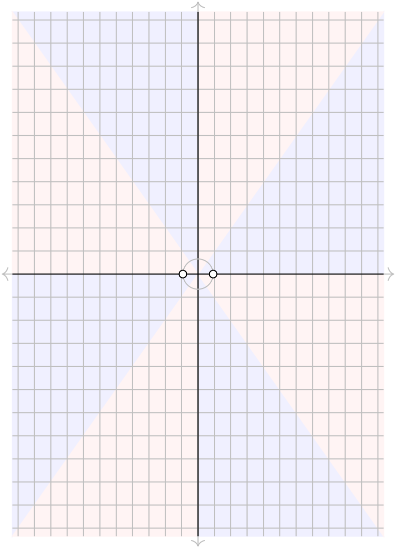
$(R/I)/(J/I) \cong R/J \cong \mathbb{Z}_2^2$

Primes in $R_{-5} = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ (Chapter 9)

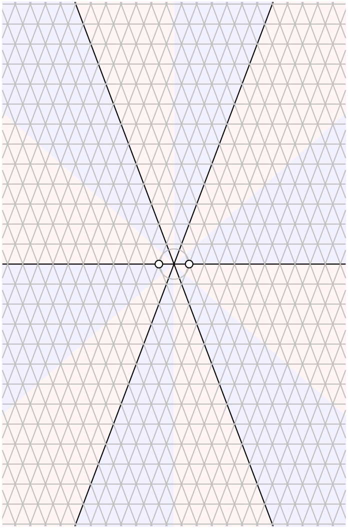
Units are white, primes are **black**, non-prime irreducibles are **blue**, **red** and **purple**.



Quadratic integer rings (Chapter 9)



"$R_{-2} = \mathbb{Z}[\sqrt{-2}]$ is *rectangular*"

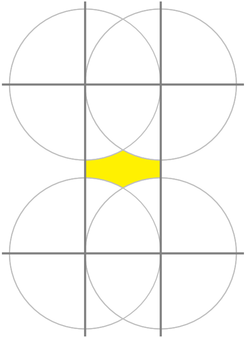


"$R_{-7} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ is *triangular*"

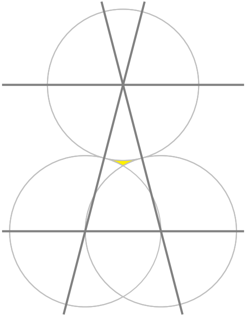
Fact

For $m < 0$, the ring R_m is norm-Euclidean iff the unit balls centered at points in R_m cover the complex plane.

$R_{-5} = \mathbb{Z}[\sqrt{-5}]$

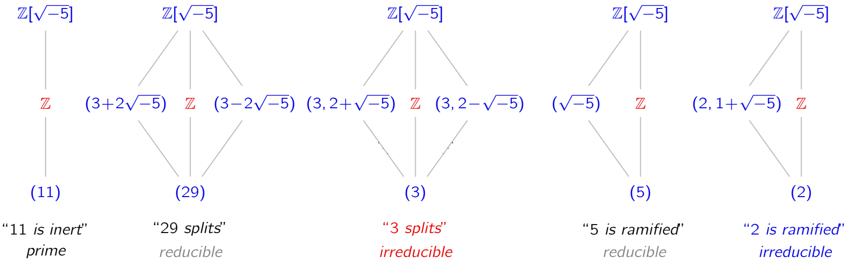


$R_{-15} = \mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$



Consider a prime $p \in \mathbb{Z}$ but in the larger ring R_m. There are three possible behaviors:

- p **splits** if $(p) = \mathfrak{p}\mathfrak{q}$
- p is **inert** if (p) remains prime
- p is **ramified** if $(p) = \mathfrak{p}^2$.

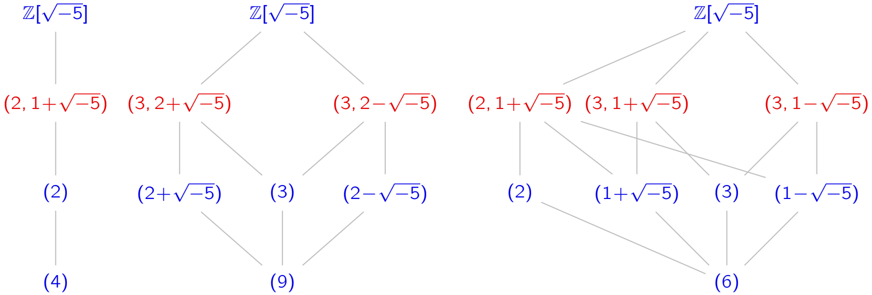


Some class field theory (Chapter 9)

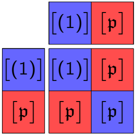
The class group, $\mathrm{Cl}(R)$, measuers how unique factorization fails in R.

It fails tamely in $R_{-5} = \mathbb{Z}[\sqrt{-5}]$

$$2 \cdot 3 = 6 = (1-\sqrt{-5})(1+\sqrt{-5}), \qquad 3 \cdot 3 = 9 = (2-\sqrt{-5})(2+\sqrt{-5}).$$

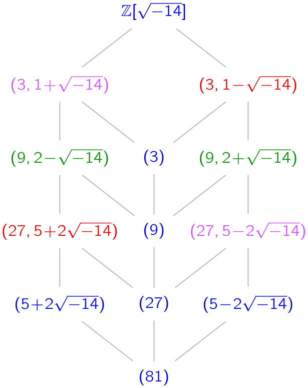


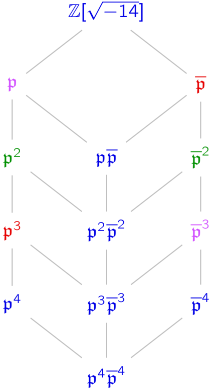
The class group is $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) \cong C_2$.



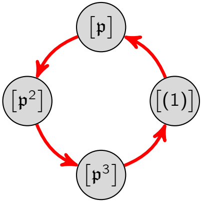
Unique factorization fails more spectacularly in $R_{-14} = \mathbb{Z}[\sqrt{-14}]$:

$$3^4 = 81 = (5+\sqrt{-14})(5-\sqrt{-14}).$$

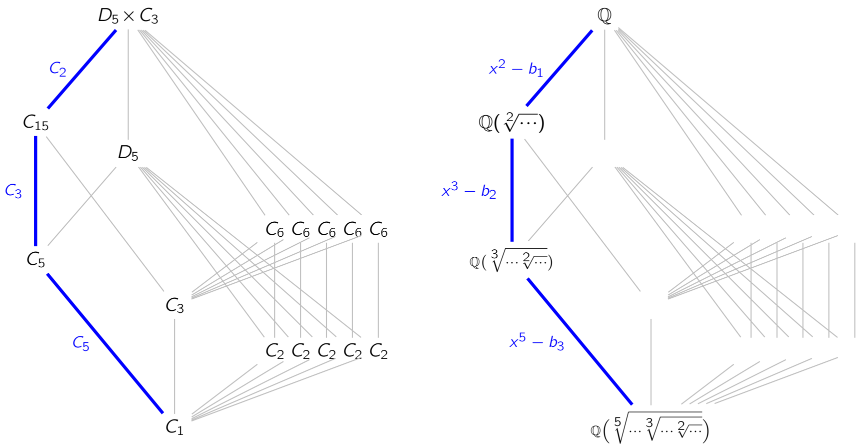


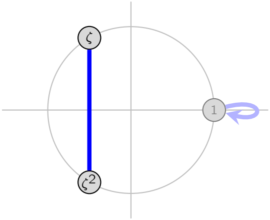


	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$	$[\mathfrak{p}^3]$
$[(1)]$	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$	$[\mathfrak{p}^3]$
$[\mathfrak{p}]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$	$[\mathfrak{p}^3]$	$[(1)]$
$[\mathfrak{p}^2]$	$[\mathfrak{p}^2]$	$[\mathfrak{p}^3]$	$[(1)]$	$[\mathfrak{p}]$
$[\mathfrak{p}^3]$	$[\mathfrak{p}^3]$	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$

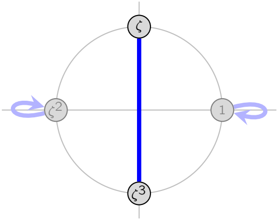


The class group is $\mathrm{Cl}(\mathbb{Z}[\sqrt{-14}]) \cong C_4$.

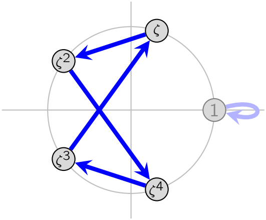

$D_5 \times C_3$
C_2
C_{15}
D_5
C_3
C_6 C_6 C_6 C_6 C_6
C_5
C_3
C_5
C_2 C_2 C_2 C_2 C_2
C_1
$\mathbb{Q}$
$x^2 - b_1$
$\mathbb{Q}(\sqrt[2]{\cdots})$
$x^3 - b_2$
$\mathbb{Q}(\sqrt[3]{\cdots\sqrt[2]{\cdots}})$
$x^5 - b_3$
$\mathbb{Q}(\sqrt[5]{\cdots\sqrt[3]{\cdots\sqrt[2]{\cdots}}})$



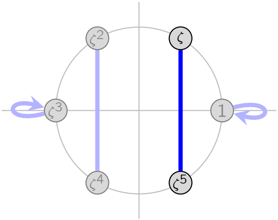
$\langle (12) \rangle \cong C_2$



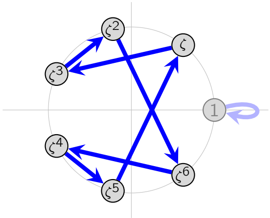
$\langle (13) \rangle \cong C_2$



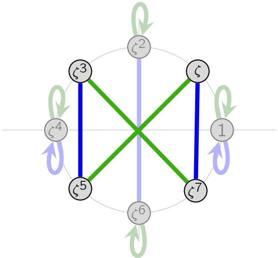
$\langle (1243) \rangle \cong C_4$



$\langle (15)(24) \rangle \cong C_2$



$\langle (132645) \rangle \cong C_6$

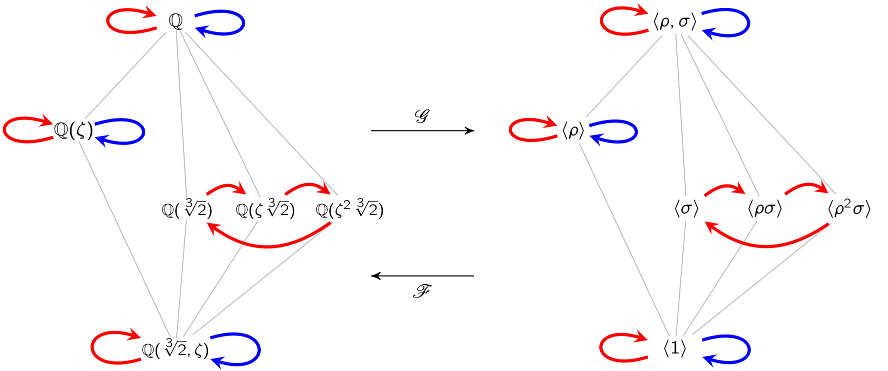


$\langle (15)(37), (17)(26)(35) \rangle \cong V_4$

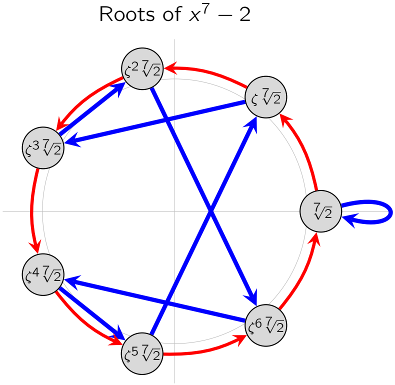
Equivalence of actions of the Galois group (Chapter 11)

The Galois group $\text{Gal}(x^3-2)$ *acts on...*

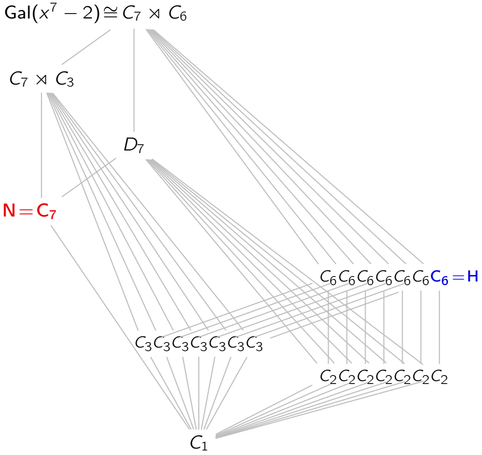
...subfields of its splitting field *...its subgroups by conjugation*



When the Galois group is a semidirect product (Chapter 11)



$\langle (1234567), (1326451) \rangle \cong C_7 \rtimes C_6 \leq S_7$



Where to learn more

- Subscribe to my YouTube channel!
- Follow @VisualAlgebra on BlueSky and Twitter/X.
- Visual Algebra webpage for slides, HW, exams:

  `http://www.math.clemson.edu/~macaule/visualalgebra.html`

- Read my articles!
  - Macauley, M. (2024). Dihedralizing the quaternions. *Amer. Math. Monthly*, **131**(4), 294–308.
  - Macauley, M. (2025). Cayley tables and lattices of finite rings. *Math. Mag.*, In press.
- Nathan Carter's *Visual Group Theory* book.
- Dana Ernst's inquiry based learning visual algebra book: `http://danaernst.com/`

Future to do list (as of December 2024)

- Finalize *Visual Algebra* and publish it.
- Finish recording *Visual Algebra* and *Graduate Visual Algebra* playlists.
- Put LaTeX files for my slides on GitHub.

Feel free to get in touch!

THANK YOU!!!