Visual Algebra

Lecture 2.11: Groups of matrices

Dr. Matthew Macauley

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

Groups of matrices

Definition

A group G is linear if it is isomorphic to a group of matrices.

We also say that G is represented by matrices.

The branch of mathematics that studys this is representation theory.

By Cayley's theorem, every finite group can be represented with permutation matrices.

We've seen how to represent a number of groups with 2×2 matrices:

- the Klein 4-group
- cyclic groups
- dihedral groups
- quaternion groups
- dicyclic groups
- diquaternion groups
- semidihedral groups
- semiabelian groups

$$\underbrace{\begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}}_{R_n}, \quad \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{F}, \quad \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{J},$$

The group $\langle a, b \mid ab^2a^{-1} = b^3 \rangle$ is not linear.

Braid groups

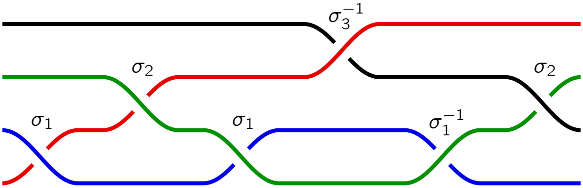
Definition

The braid group is defined by the presentation

$$\textbf{Braid}_n = \Big\langle \sigma_1, \ldots, \sigma_{n-1} \;\Big|\; \underbrace{\sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| \geq 2}_{\textit{Type I relation}}, \quad \underbrace{\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}}_{\textit{Type II relation}} \Big\rangle.$$

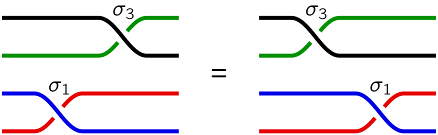
Here is the element

$$\sigma_1\sigma_2\sigma_1\sigma_3^{-1}\sigma_1^{-1}\sigma_2 = \sigma_1\sigma_2\sigma_3^{-1}\sigma_2 \in \textbf{Braid}_4 = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$$

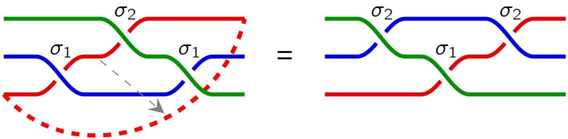


Braid groups

The braid relations come from the following easy-to-verify properties of physical braids:



$$\sigma_i \sigma_j = \sigma_j \sigma_i$$
$$(\text{if } |i-j| \geq 2)$$



$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$$

For 70 years, it was unknown if braid groups were linear.

Theorem (Bigelow, 2000; Krammer, 2002)

Braid groups are linear.

Groups of matrices

Matrices are a rich source of groups in their own right.

Let's define a few terms so we can better speak of certain sets of matrices.

Square matrices are objects that we can add, subtract, and multiply, but not always divide.

Definition

A ring is an abelian group R that is additionally

- closed under multiplication, and
- satisfies the distributive property.

If we can also divide by any nonzero element, it is a field, $\mathbb{F}$.

Some rings contain zero divisors: two nonzero x, y such that $xy = 0$.

For example, $2 \cdot 3 = 0$ in $\mathbb{Z}_6$.

In other rings, multiplication does not commute.

Henceforth, we will usually assume that our matrix coefficients m_{ij} come from a field $\mathbb{F}$.

Basically, we're intersted in examples like $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, etc.

Groups of matrices

The set $\mathrm{Mat}_{n,m}(\mathbb{F})$ of $n \times m$ matrices is a group under addition, but a very boring one.

It is isomorphic to the direct product $\mathbb{F}^{mn} := \mathbb{F} \times \cdots \times \mathbb{F}$ of nm copies of $\mathbb{F}$.

It is more interesting to look at groups of square matrices under multiplication.

Definition

Let $\mathrm{Mat}_n(\mathbb{F})$ be the set of $n \times n$ matrices with coefficients from $\mathbb{F}$.

Since matrices represent linear transformation, many standard matrix groups have "*linear*" in their names.

Definition

Thqe general linear group of degree n over R is the set of invertible matrices with coefficients from R:

$$\mathrm{GL}_n(R) = \left\{A \in \mathrm{Mat}_n(R) \mid \det A \neq 0\right\}.$$

The special linear group is the subgroup of matrices with determinant 1:

$$\mathrm{SL}_n(R) = \left\{A \in \mathrm{GL}_n(R) \mid \det A = 1\right\}.$$

An interesting group of order 24

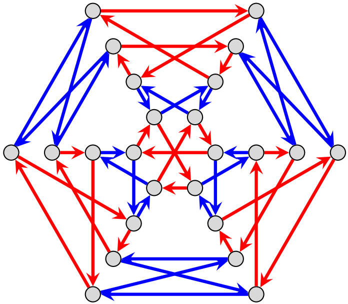
Some interesting finite groups arise as special or general linear groups over $\mathbb{Z}_q$. For example,

$$\mathsf{SL}_2(\mathbb{Z}_3) = \langle A, B \mid A^3 = B^3 = (AB)^2 \rangle = \langle A, B, C \mid A^3 = B^3 = C^2 = CAB \rangle \cong Q_8 \rtimes \mathbb{Z}_3,$$

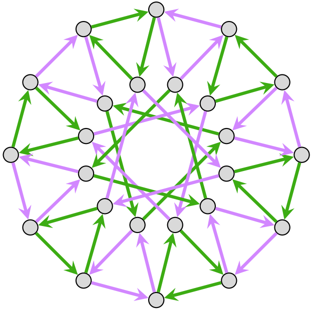
and the matrices A and B can be taken to be

$$A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}, \qquad B = \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix}.$$

Here are Cayley graphs for different generating sets:



$\langle R, S \mid R^6 = S^4 = (RS)^3 = I \rangle$



$\langle x, y \mid x^3 = y^3 = (xy)^3 = 1 \rangle$

The Hamiltonians

The group $\mathrm{SL}_2(\mathbb{Z}_3)$ can be represented with quaternions. The Hamiltonians are the ring

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

One way to represent these is with 2×2 matrices over $\mathbb{C}$:

$$\mathbb{H} \cong \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} : z, w \in \mathbb{C} \right\} = \left\{ \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

Yet another way involves 4×4 matrices over $\mathbb{R}$:

$$\mathbb{H} \cong \left\{ \begin{bmatrix} a & b & -d & -c \\ -b & a & -c & d \\ d & c & a & b \\ c & -d & -b & a \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

Removing 0 from $\mathbb{H}$ defines a multiplicative group $\mathbb{H}^*$ with lots of interesting subgroups.

One of them is the unit quaternions, which physicists assoiciate with points in a 3-sphere:

$$S^3 := \{a + bi + cj + dk \mid a^2 + b^2 + c^2 + d^2 = 1\}.$$

The group $\mathrm{SL}_2(\mathbb{Z}_3)$ is isomorphic to a subgroup called the binary tetrahedral group,

$$\mathrm{SL}_2(\mathbb{Z}_3) \cong 2\mathrm{T} := \{ \pm 1, \pm i, \pm j, \pm k, \tfrac{1}{2}(\pm 1 \pm i \pm j \pm k)\} \le S^3.$$

Finite subgroups of $SL_2(\mathbb{C})$

The binary triangle group with parameters (p, q, r) is

$$\Gamma(p,q,r) = \left\langle a, b, c \mid a^p = b^q = c^r = abc \right\rangle.$$

Theorem

Every finite subgroup of $SL_2(\mathbb{C})$ is isomorphic to one of the following:

- cyclic group of order n: $C_n = \langle \zeta_n \rangle$
- binary dihedral group $\Gamma(2,2,n)$ of order $4n$: $\langle \zeta_{2n}, j \rangle \cong \mathrm{Dic}_{2n}$
- binary tetrahedral group $\Gamma(2,3,3)$ of order 24:

$$2\mathrm{T} = \left\langle i, j, \tfrac{1}{2}(1+i-j+k) \right\rangle \cong SL_2(\mathbb{Z}_3)$$

- binary octahedral group $\Gamma(2,3,4)$ of order 48:

$$2\mathrm{O} = \left\langle \tfrac{1+i}{\sqrt{2}}, j, \tfrac{1}{2}(1+i-j+k) \right\rangle$$

- binary icosahedral group $\Gamma(2,3,5)$ of order 120:

$$2\mathrm{I} = \left\langle j, \tfrac{1}{2}(1+i+j+k), \tfrac{1}{2}(\phi+\phi^{-1}i+j) \right\rangle \cong SL_2(\mathbb{Z}_5).$$

Matrix groups over other finite fields

The group $\mathsf{GL}_n(\mathbb{Z}_p)$ consists of the linear maps of the vector space $\mathbb{Z}_p^n$ to itself.

Each one is determined by an ordered basis $v_1, \dots, v_n$ of $\mathbb{Z}_p^n$.

Let's count these. There are:

1. $p^n - 1$ choices for v_1, then
2. $p^n - p$ choices for v_2, then
3. $p^n - p^2$ choices for v_3, and so on...

n. $p^n - p^{n-1}$ choices for v_n.

Therefore,

$$\big|\,\mathsf{GL}_n(\mathbb{Z}_p)\big| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}).$$

These groups have many subgroups, and they often happen to coincide with familiar groups that we have seen.

For example, by "dumb luck",

$$D_9 \cong \left\langle \begin{bmatrix} 16 & 10 \\ 7 & 14 \end{bmatrix}, \begin{bmatrix} 14 & 6 \\ 10 & 3 \end{bmatrix} \right\rangle \leq \mathsf{GL}_2(\mathbb{Z}_{17}), \qquad \mathrm{Dic}_{12} \cong \left\langle \begin{bmatrix} 2 & 7 \\ 7 & 3 \end{bmatrix}, \begin{bmatrix} 0 & 10 \\ 1 & 0 \end{bmatrix} \right\rangle \leq \mathsf{GL}_2(\mathbb{Z}_{11}).$$

GroupNames online database

metacyclic, supersoluble, monomial, Z-group, 2-hyperelementary

Aliases: D_9, $C_9{:}C_2$, $C_3.S_3$, sometimes denoted D_{18} or Dih_9 or Dih_{18}, SmallGroup(18,1)

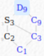
Series: Derived ▸Chief ▸Lower central ▸Upper central

Derived series C_1 — C_9 — D_9

Generators and relations for D_9

$G = \langle a,b \mid a^9=b^2=1, bab=a^{-1} \rangle$

Subgroups: 16 in 6 conjugacy classes, 4 normal (all characteristic)
Quotients: C_1, C_2, S_3, D_9



Character table of D_9

class	1	2	3	9A	9B	9C	
size	1	9	2	2	2	2	
ρ_1	1	1	1	1	1	1	trivial
ρ_2	1	-1	1	1	1	1	linear of order 2
ρ_3	2	0	2	-1	-1	-1	orthogonal lifted from S_3
ρ_4	2	0	-1	$\zeta_9^5+\zeta_9^4$	$\zeta_9^7+\zeta_9^2$	$\zeta_9^8+\zeta_9$	orthogonal faithful
ρ_5	2	0	-1	$\zeta_9^8+\zeta_9$	$\zeta_9^5+\zeta_9^4$	$\zeta_9^7+\zeta_9^2$	orthogonal faithful
ρ_6	2	0	-1	$\zeta_9^7+\zeta_9^2$	$\zeta_9^8+\zeta_9$	$\zeta_9^5+\zeta_9^4$	orthogonal faithful

Permutation representations of D_9

▸On 9 points - transitive group 9T3
▸Regular action on 18 points - transitive group 18T5

D_9 is a **maximal subgroup of**

$C_9{:}C_6$ $C_9{:}S_3$ $C_3.S_4$ $C_3^2{:}D_9$
D_{9p}: D_{27} D_{45} D_{63} D_{99} D_{117} D_{153} D_{171} D_{207} ...

D_9 is a **maximal quotient of**

$C_9{:}S_3$ $C_3.S_4$ $C_3^2{:}D_9$
$C_{3p}.S_3$: Dic_9 D_{27} D_{45} D_{63} D_{99} D_{117} D_{153} D_{171} ...

Polynomial with Galois group D_9 over Q

action	f(x)	Disc(f)
9T3	$x^9+3x^8-67x^7-226x^6+699x^5+1211x^4-3137x^3+940x^2+904x-392$	$2^{22}\cdot 7^4\cdot 13^2\cdot 19^6\cdot 29^2\cdot 229^4\cdot 547^2$

Matrix representation of D_9 ▸in $GL_2(\mathbb{F}_{17})$ generated by

$$\begin{bmatrix}16&10\\7&14\end{bmatrix},\begin{bmatrix}14&6\\10&3\end{bmatrix}$$

metacyclic, supersoluble, monomial, 2-hyperelementary

Aliases: Dic_6, $C_3\rtimes Q_8$, $C_4.S_3$, $C_2.D_6$, $C_{12}.C_2$, $Dic_3.C_2$, $C_6.C_2^2$, SmallGroup(24,4)

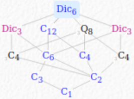
Series: Derived ▸Chief ▸Lower central ▸Upper central

Derived series C_1 — C_6 — Dic_6

Generators and relations for Dic_6

$G = \langle a,b \mid a^{12}=1, b^2=a^6, bab^{-1}=a^{-1} \rangle$

Subgroups: 18 in 12 conjugacy classes, 9 normal (7 characteristic)
Quotients: C_1, C_2, C_2^2, S_3, Q_8, D_6, Dic_6



Character table of Dic_6

class	1	2	3	4A	4B	4C	6	12A	12B	
size	1	1	2	2	6	6	2	2	2	
ρ_1	1	1	1	1	1	1	1	1	1	trivial
ρ_2	1	1	1	1	-1	-1	1	1	1	linear of order 2
ρ_3	1	1	1	-1	-1	1	1	-1	-1	linear of order 2
ρ_4	1	1	1	-1	1	-1	1	-1	-1	linear of order 2
ρ_5	2	2	-1	2	0	0	-1	-1	-1	orthogonal lifted from S_3
ρ_6	2	2	-1	-2	0	0	-1	1	1	orthogonal lifted from D_6
ρ_7	2	-2	2	0	0	0	-2	0	0	symplectic lifted from Q_8, Schur index 2
ρ_8	2	-2	-1	0	0	0	1	$\sqrt{3}$	$-\sqrt{3}$	symplectic faithful, Schur index 2
ρ_9	2	-2	-1	0	0	0	1	$-\sqrt{3}$	$\sqrt{3}$	symplectic faithful, Schur index 2

Permutation representations of Dic_6

▸Regular action on 24 points - transitive group 24T5

Dic_6 is a **maximal subgroup of**

$A_4\rtimes Q_8$ $C_4.S_4$ $C_3^3\rtimes Q_8$ $CSU_2(\mathbb{F}_5)$
Dic_{6p}: Dic_{12} Dic_{18} Dic_{30} Dic_{42} Dic_{66} Dic_{78} Dic_{102} Dic_{114} ...
$C_{2p}.D_6$: $C_{24}\rtimes C_2$ $D_4.S_3$ $C_3\rtimes Q_{16}$ $C_4\circ D_{12}$ $D_4\rtimes_2 S_3$ $S_3\times Q_8$ $C_3^2\rtimes_2 Q_8$ $C_3^2\rtimes_4 Q_8$ ...

Dic_6 is a **maximal quotient of**

$A_4\rtimes Q_8$ $C_3^3\rtimes Q_8$
$C_6.D_{2p}$: $Dic_3\rtimes C_4$ $C_4\rtimes Dic_3$ Dic_{18} $C_3^2\rtimes_2 Q_8$ $C_3^2\rtimes_4 Q_8$ $C_{15}\rtimes Q_8$ Dic_{30} $C_{21}\rtimes Q_8$ ...

Matrix representation of Dic_6 ▸in $GL_2(\mathbb{F}_{11})$ generated by

$$\begin{bmatrix}2&7\\7&3\end{bmatrix},\begin{bmatrix}0&10\\1&0\end{bmatrix}$$

LMFDB: https://lmfdb.org/Groups/Abstract/

⌂ → Groups → Abstract

Abstract groups

· Login
Citation · Feedback · Hide Menu

The database currently contains 544,831 groups from many different sources, the largest of which is S_{47} of order 47!. In addition, it contains 275,379,753 of their subgroups and 39,933,457 of their irreducible complex characters. You can browse further statistics.

Learn more
- Source and acknowledgements
- Completeness of the data
- Reliability of the data
- Abstract group labeling

Browse

By order: 1-64 65-127 128 129-255 256 257-383 384 385-511 513-1000 1001-1500 1501-2000 2001-

By nilpotency class: 1 2 3 4 5 6 7 8 9 (and not nilpotent)

By property: abelian nonabelian solvable nonsolvable simple perfect rational

Some interesting groups or a random group

Search for subgroups or complex characters

Search

Advanced search options

Order	3	e.g. 4, or a range like 3..5	Exponent	2, 3, 7	e.g. 2, or list of integers like 2, 3, 7
Automorphism group	4.2	e.g. 4.2	Nilpotency class	3	e.g. 4, or a range like 3..5
Automorphism group order	3	e.g. 4, or a range like 3..5	Commutator	4.2, 8	e.g. 4 or 4.2 (order or label)
Center	4.2, 8	e.g. 4 or 4.2 (order or label)	Abelianization	4.2, 8	e.g. 4 or 4.2 (order or label)
Central quotient	4.2, 8	e.g. 4 or 4.2 (order or label)			
Abelian			Direct product		
Cyclic			Semidirect product		
Nilpotent			Perfect		
Simple			Solvable		
Transitive degree	3	e.g. 4, or a range like 3..5	Permutation degree	3	e.g. 4, or a range like 3..5
Number of subgroups	3	e.g. 4, or a range like 3..5	Number of normal subgroups	3	e.g. 4, or a range like 3..5
Number of conjugacy classes	3	e.g. 4, or a range like 3..5			
Order statistics	1^1, 2^3, 3^2	e.g. 1^1, 2^3, 3^2			
Results to display	50				

Display: List of groups | Random group

Affine groups

Let V be a vector space over a $\mathbb{F}$. A map $L\colon V \to V$ is linear if

$$L(c\mathbf{x} + d\mathbf{y}) = cL\mathbf{x} + dL\mathbf{y}, \qquad \text{for all } x, y \in V \text{ and } c, d \in \mathbb{F}.$$

If $\dim V = n < \infty$, we can write this with an $n \times n$ matrix.

Key point

- A linear map $f\colon V \to V$ has the form $f(\mathbf{x}) = A\mathbf{x}$.
- An affine map $f\colon V \to V$ has the form $f(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$.

The 1-dimensional general affine group over a field $\mathbb{F}$ as

$$\mathrm{AGL}_1(\mathbb{F}) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{F},\ a \neq 0 \right\}.$$

The 2-dimensional general affine group can be defined as

$$\mathrm{AGL}_2(\mathbb{F}) = \left\{ \begin{bmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ 0 & 0 & 1 \end{bmatrix} : a_{ij}, b_j \in \mathbb{F},\ a_{11}a_{22} - a_{12}a_{21} \neq 0 \right\}.$$

We can encode an affine map of an n-dimensional space V as an $(n+1) \times (n+1)$ matrix:

$$\mathbf{y} = f(\mathbf{x}) = A\mathbf{x} + \mathbf{b}, \qquad \text{as} \qquad \begin{bmatrix} \mathbf{y} \\ 1 \end{bmatrix} = \begin{bmatrix} A & \mathbf{b} \\ \mathbf{0} & 1 \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ 1 \end{bmatrix}.$$