# What are...matrix groups?

Or: The most important groups?!

## Producing groups

Automorphisms of $X$ form a group $\mathrm{Aut}(X)$:

- Multiplication is composition of maps Multiplication
- Composition of maps is associative Associativity
- The identity map is a do nothing operation Unit
- Automorphism are invertible Inverse

---

- $\mathrm{Aut}$(finite sets) give symmetric groups
- $\mathrm{Aut}$(field extensions) give Galois groups (roots of polynomials)
- $\mathrm{Aut}(\mathbb{K}$ vector spaces) give $\mathrm{GL}_n(\mathbb{K})$
- $\mathrm{Aut}(\mathbb{K}$ projective spaces) give $\mathrm{PGL}_n(\mathbb{K})$

# Producing finite groups

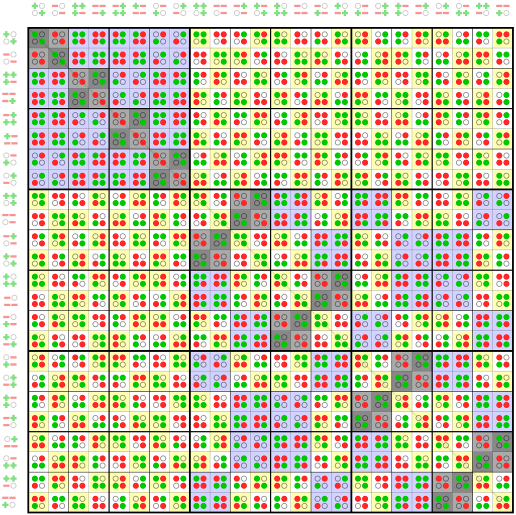
Multiplication table of $\mathrm{GL}_2(\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z})$ (white=0, black=1):

| | $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ | $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ |
|---|---|---|---|---|---|---|
| $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ | $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ | $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ |
| $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ | $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ |
| $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ | $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ |
| $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ | $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ |
| $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ | $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ |
| $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ | $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ | $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ | $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ | $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ |

Small number coincidence: this is $S_3$

# Producing finite groups

Multiplication table of $\mathrm{SL}_2(\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z})$ (white=0, green=1, red=2):



This is a group of order 24

## For completeness: A formal statement

A variant of Cayley's theorem. A finite group $G$ of order $n$ can be realized as a subgroup of $\mathrm{GL}_n(\mathbb{Z})$

Proof idea. From the multiplication table of a finite group one gets matrices, *e.g.*

| $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ | $(0,0)$ | $(1,0)$ | $(0,1)$ | $(1,1)$ |
|---|---|---|---|---|
| $(0,0)$ | $(0,0)$ | $(1,0)$ | $(0,1)$ | $(1,1)$ |
| $(1,0)$ | $(1,0)$ | $(0,0)$ | $(1,1)$ | $(0,1)$ |
| $(0,1)$ | $(0,1)$ | $(1,1)$ | $(0,0)$ | $(1,0)$ |
| $(1,1)$ | $(1,1)$ | $(0,1)$ | $(1,0)$ | $(0,0)$ |

$\Rightarrow$

$$(0,0)\mapsto \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}$$

$$(1,0)\mapsto \begin{pmatrix} 0&1&0&0\\ 1&0&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix}$$

$$(0,1)\mapsto \begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{pmatrix}$$

$$(1,1)\mapsto \begin{pmatrix} 0&0&0&1\\ 0&0&1&0\\ 0&1&0&0\\ 1&0&0&0 \end{pmatrix}$$

Subgroups of matrices are called linear groups

All finite groups are linear

but not all groups are linear

# Finite groups from matrices – continued

- $\mathrm{GL}_n(\mathbb{F}_q)$ is a finite group of order

$$|\mathrm{GL}_n(\mathbb{F}_q)| = \prod_{k=0}^{n-1}(q^n - q^k)$$

  so *e.g.* $|\mathrm{GL}_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)$
- $\mathrm{SL}_n(\mathbb{F}_q)$ is a finite group of order

$$|\mathrm{SL}_n(\mathbb{F}_q)| = \frac{1}{q-1}|\mathrm{GL}_n(\mathbb{F}_q)|$$

  so *e.g.* $|\mathrm{SL}_2(\mathbb{F}_q)| = (q+1)(q^2-q)$
- $\mathrm{O}_n(\mathbb{F}_q)$ is a finite group
- $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ is a finite group
- *etc.*

$\mathrm{GL}_n(\mathbb{F}_q)$ was one of the first groups formally discovered (by Galois $\sim$1832)

**Thank you for your attention!**

---

I hope that was of some help.