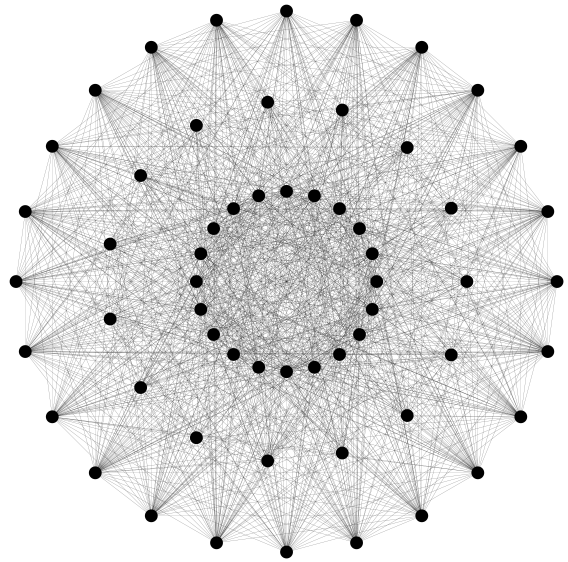
# Group Generation Through the Generations

Scott Harper

University of Bristol



St Andrews University Mathematics Society

3rd March 2017

# So what do you do?

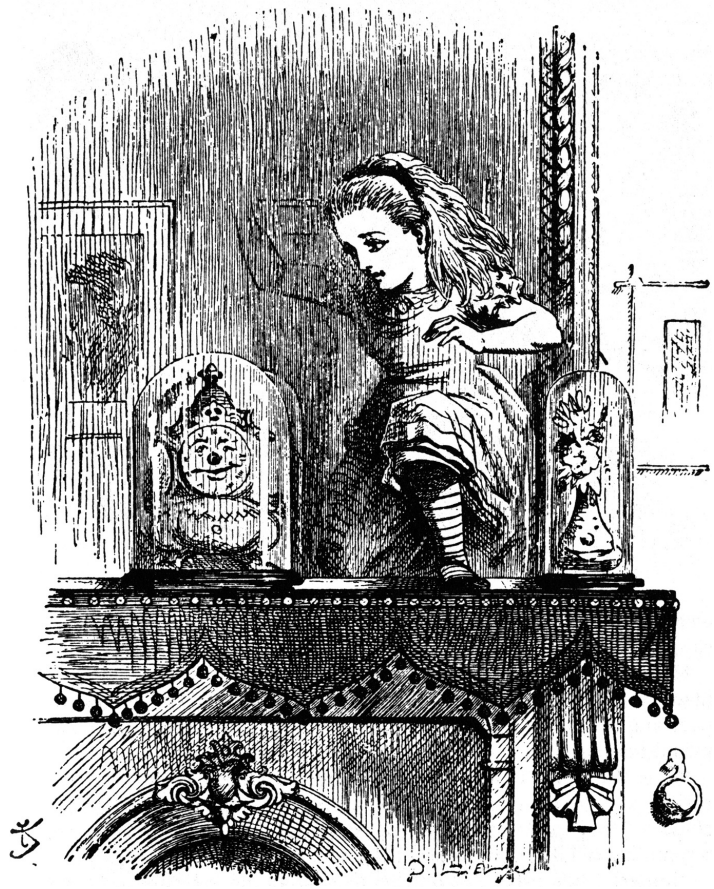
# So what do you do?

the art of measuring symmetry

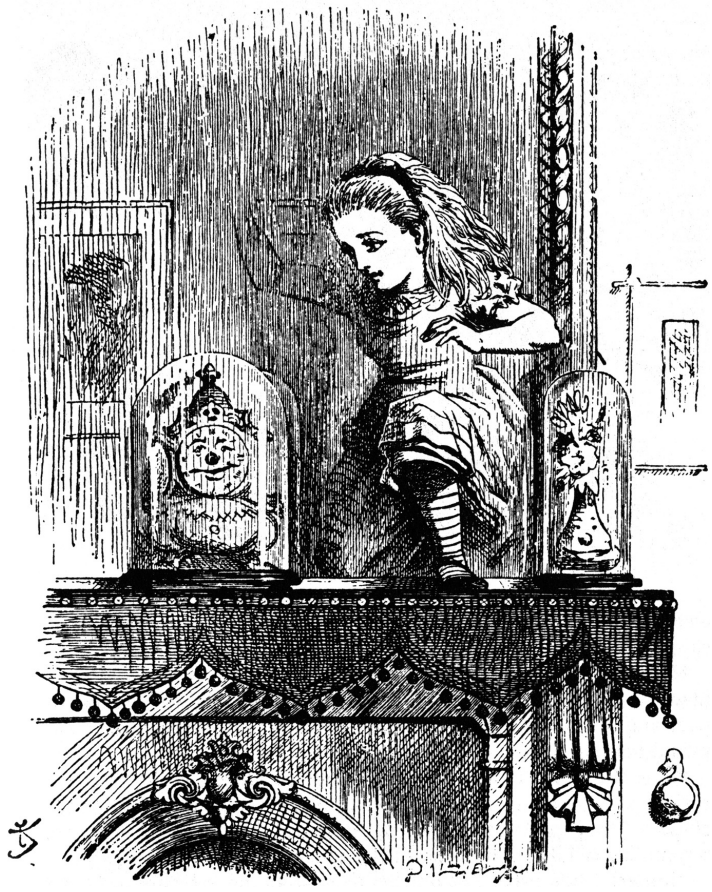
# So what do you do?

the art of measuring symmetry

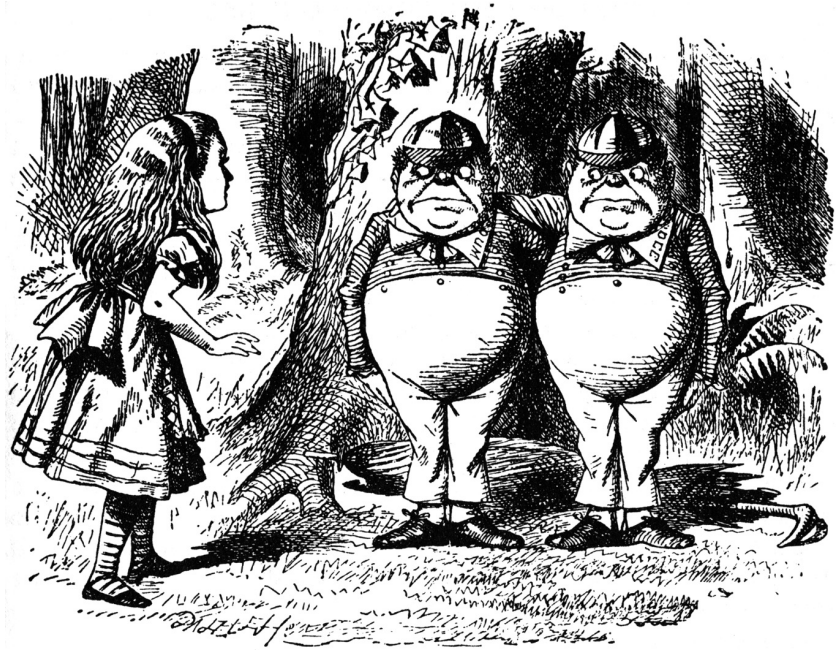
*‘Perhaps Looking-Glass milk isn’t good to drink?’*



*'Perhaps Looking-Glass milk isn't good to drink?'*

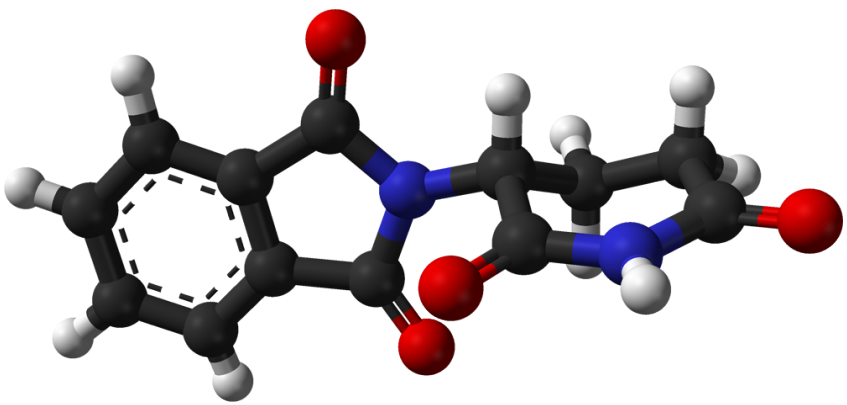


*Alice knew which was which in a moment.*

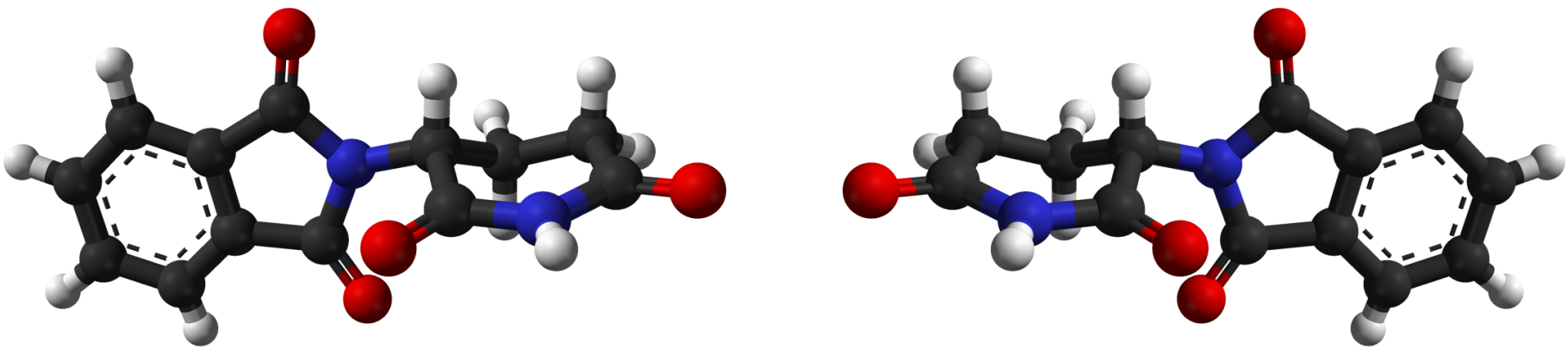


thalidomide

# thalidomide

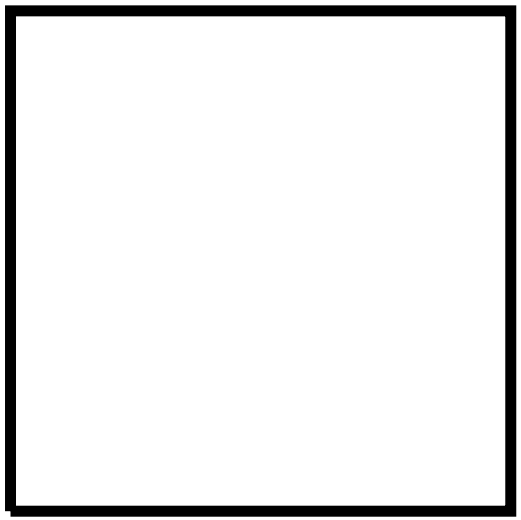


# thalidomide

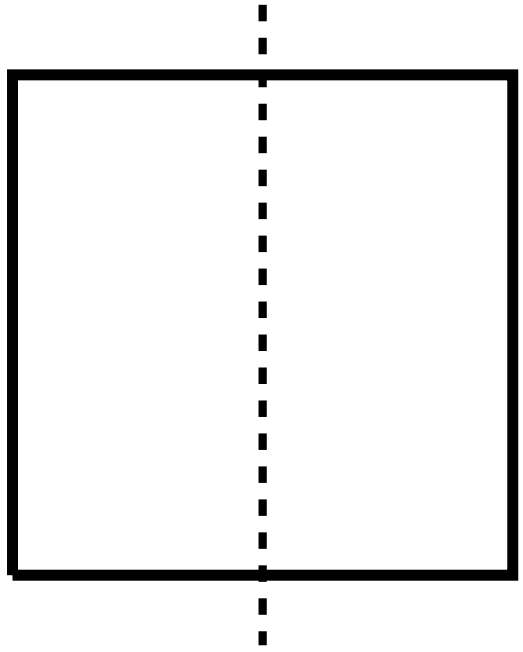


# Examples of Groups

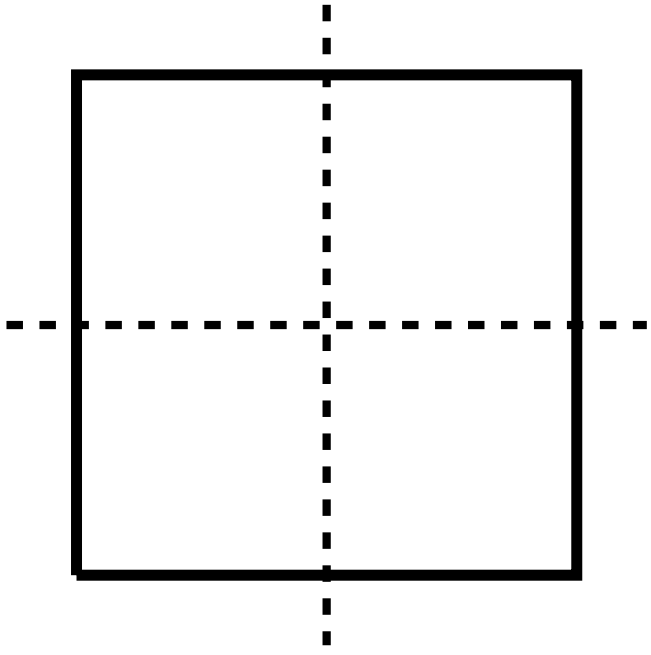
# Examples of Groups



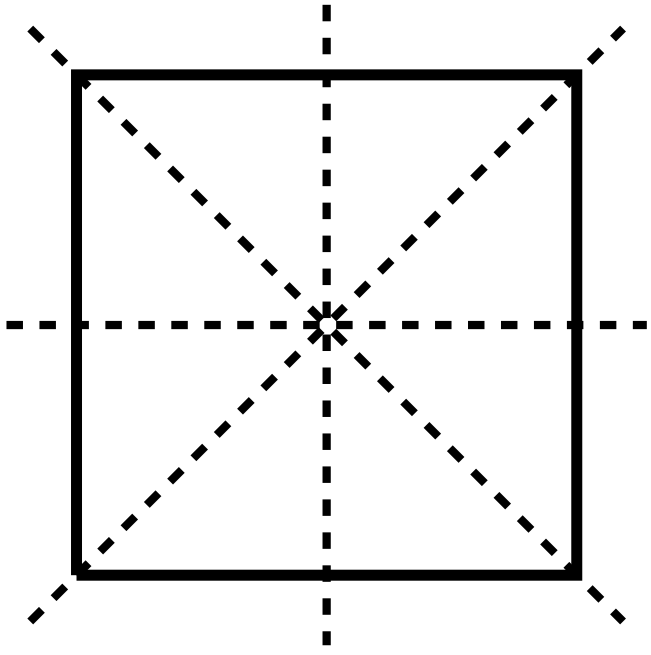
# Examples of Groups



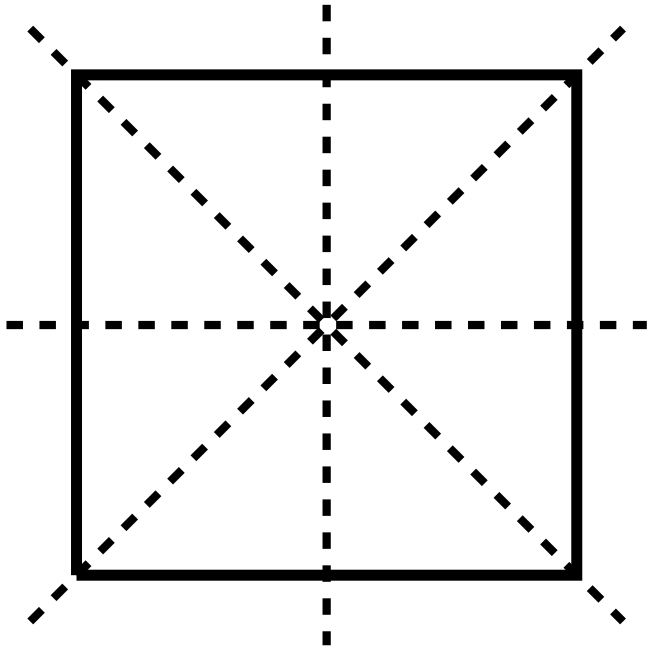
# Examples of Groups



# Examples of Groups

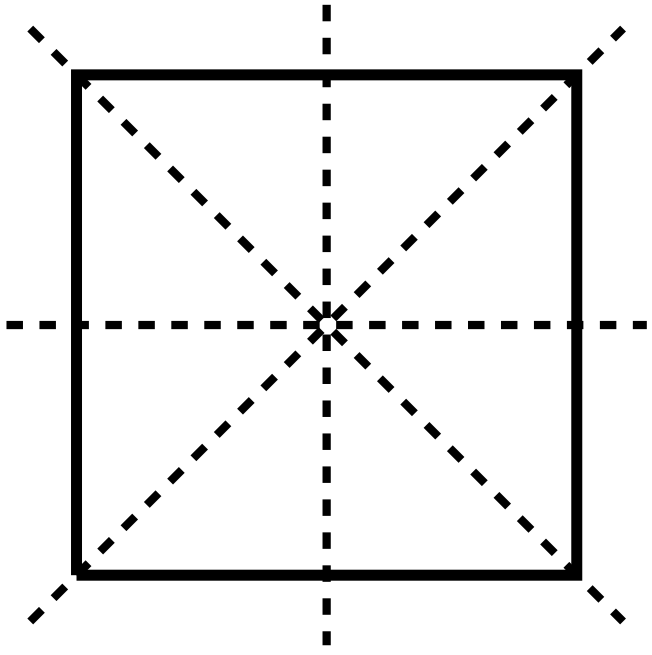


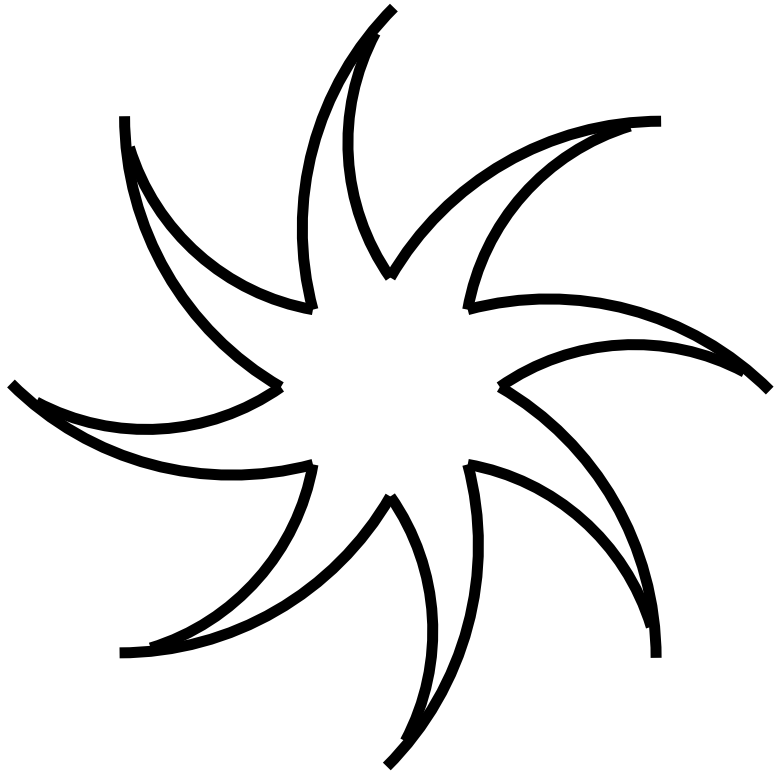
# Examples of Groups



the dihedral group $D_{\square}$

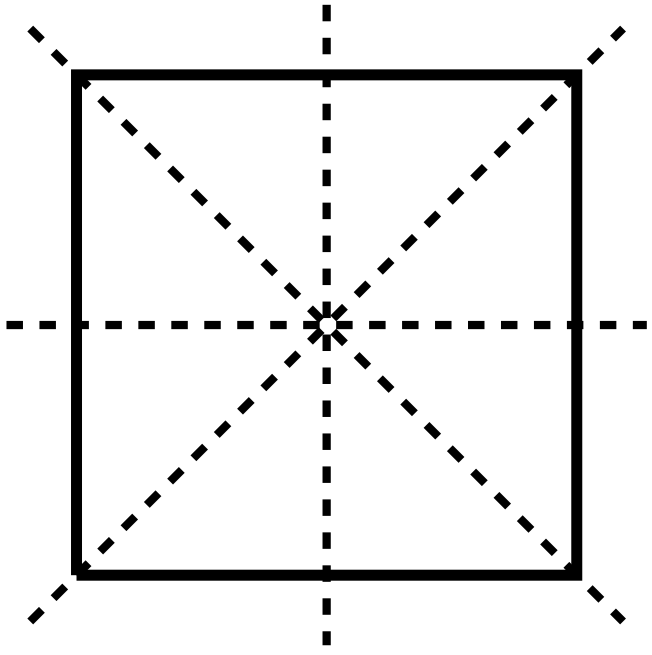
# Examples of Groups



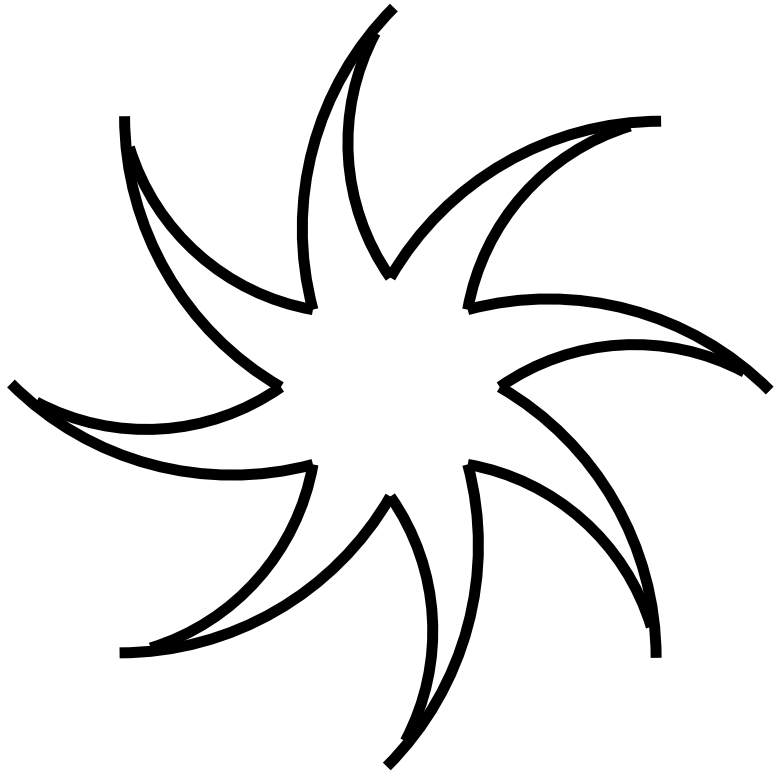


the dihedral group $D_{\square}$

# Examples of Groups

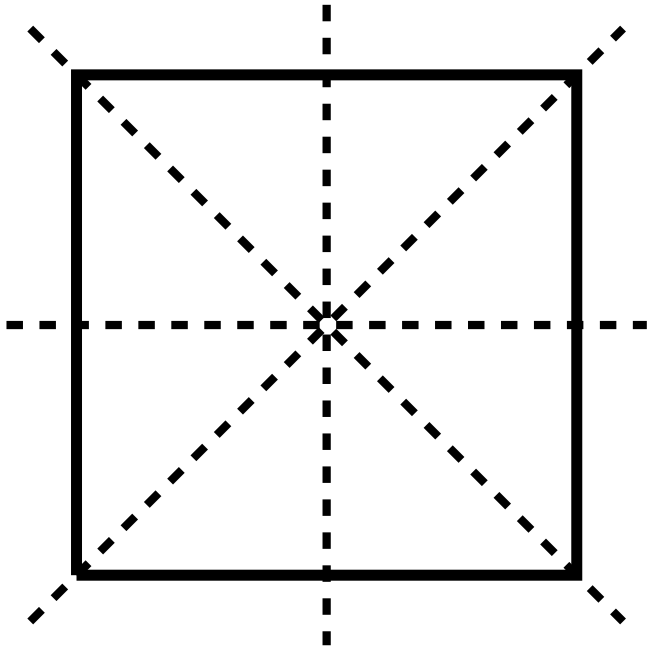


the dihedral group $D_{\square}$

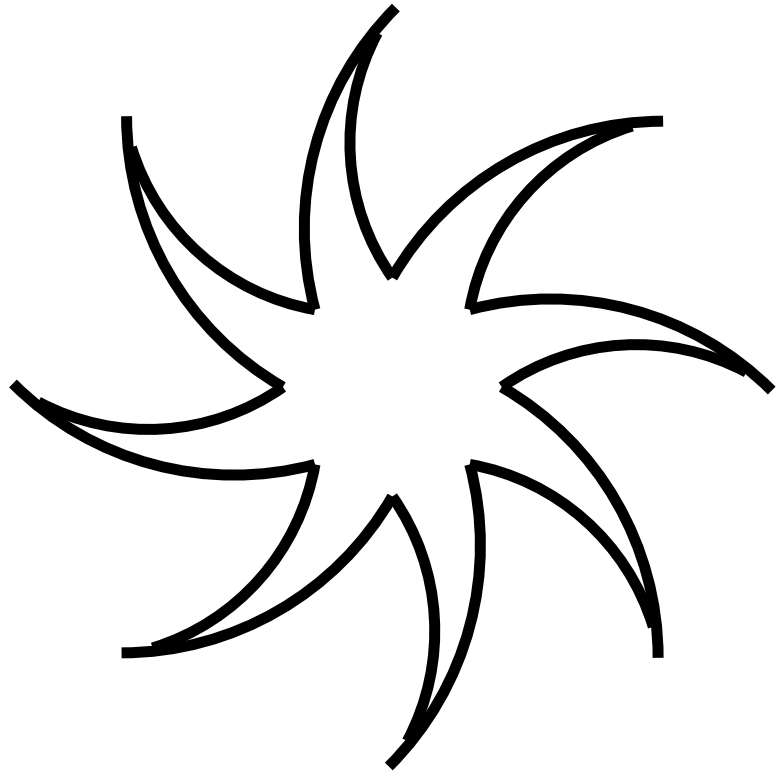


the cyclic group $C_8$

# Examples of Groups



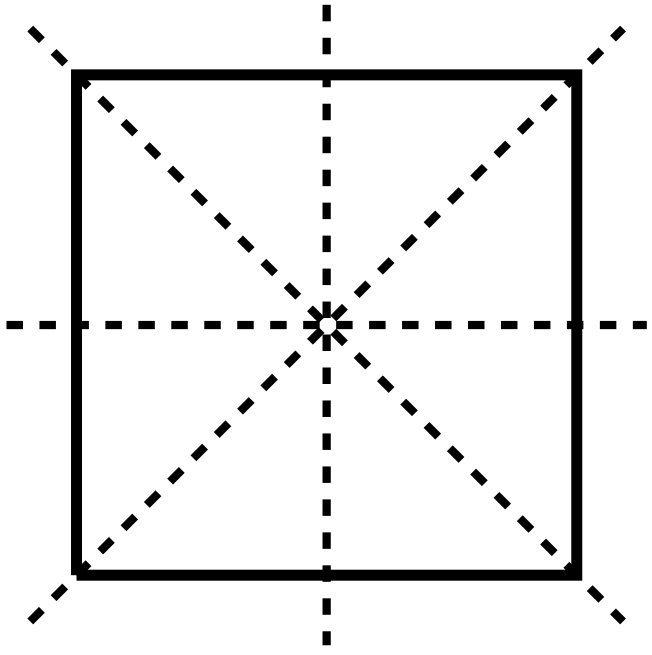
the dihedral group $D_{\square}$



the cyclic group $C_8$

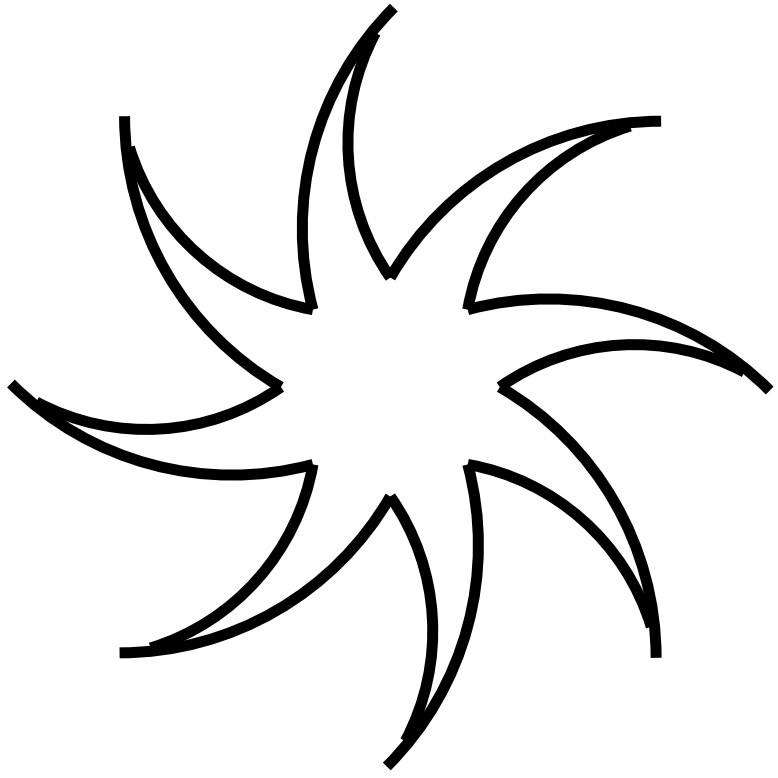
generated by one element

# Examples of Groups



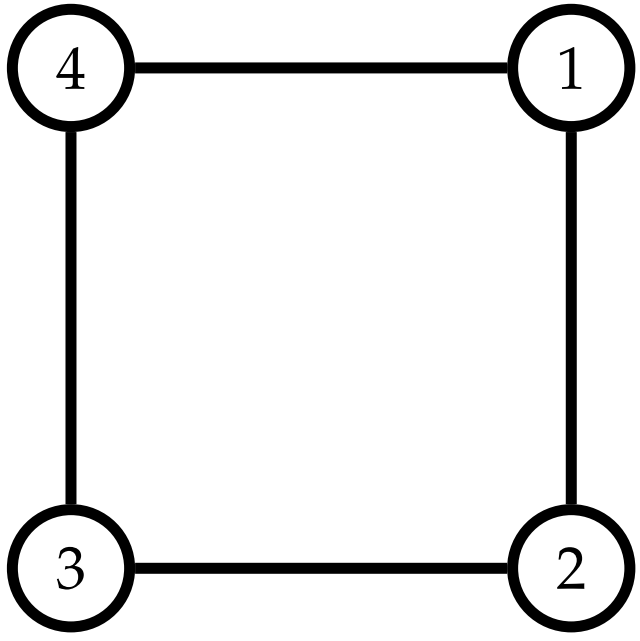
the dihedral group $D_{\square}$

generated by two elements

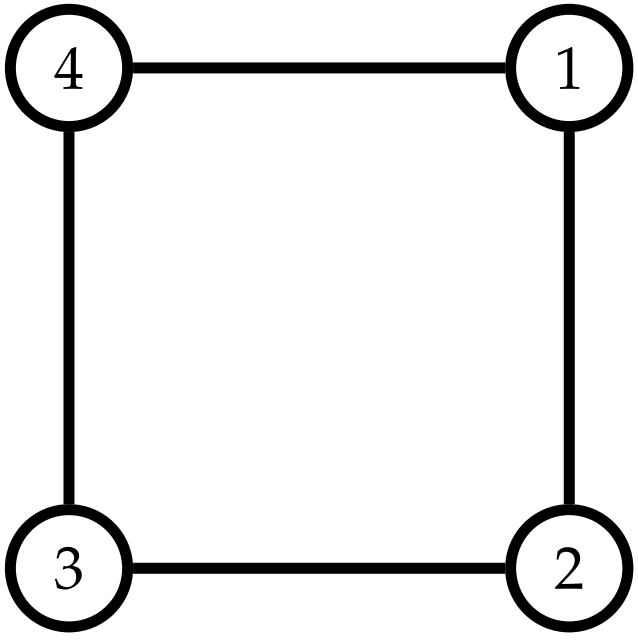


the cyclic group $C_8$

generated by one element

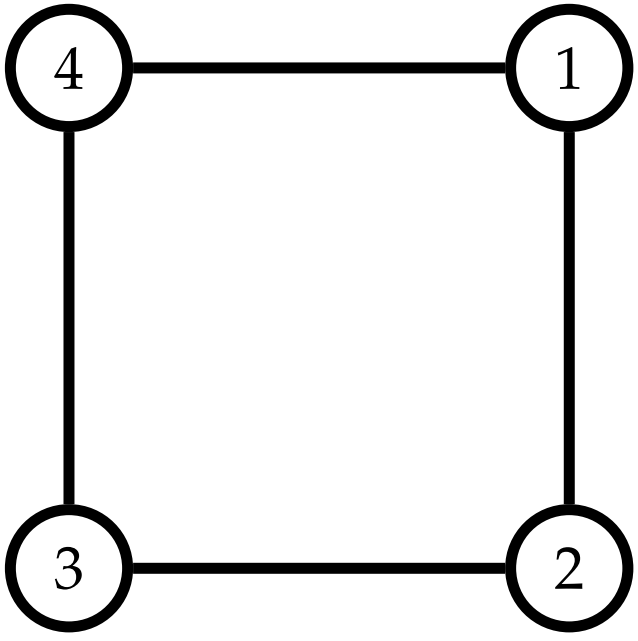



the dihedral group $D_{\square}$




Rotation by 90° clockwise

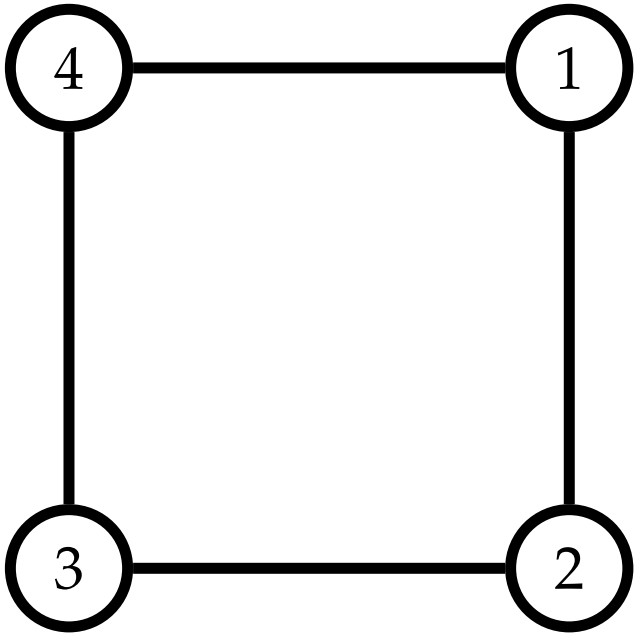
the dihedral group $D_{\square}$




the dihedral group $D_{\square}$

Rotation by 90° clockwise

$$\rho = 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto$$

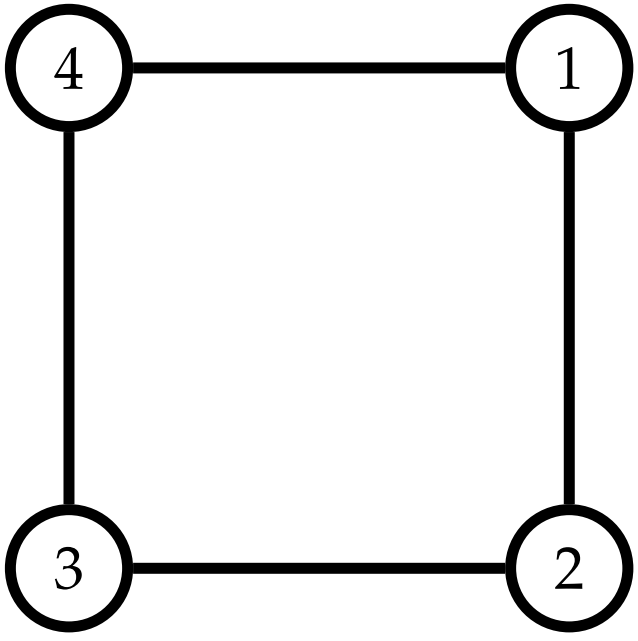



the dihedral group $D_{\square}$

Rotation by 90° clockwise

$$\rho = 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto$$

$$= (1\,2\,3\,4)$$

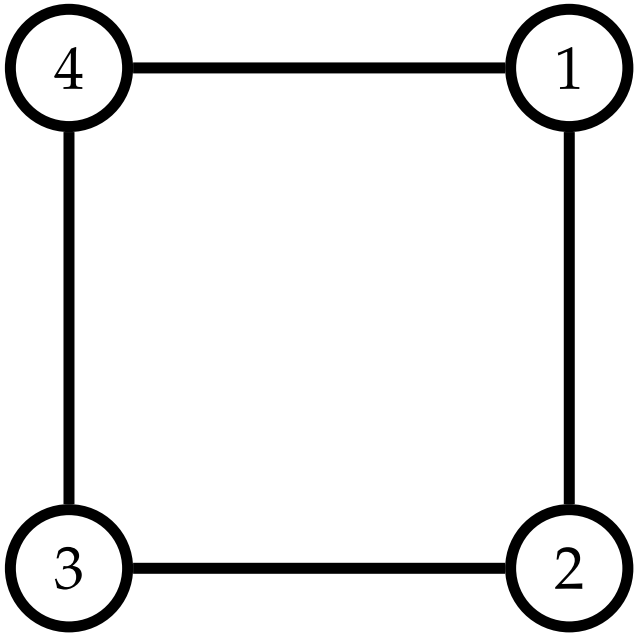



the dihedral group $D_{\square}$

Rotation by 90° clockwise

$$\rho = 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto$$
$$= (1\,2\,3\,4)$$

Reflection in vertical line




the dihedral group $D_{\square}$

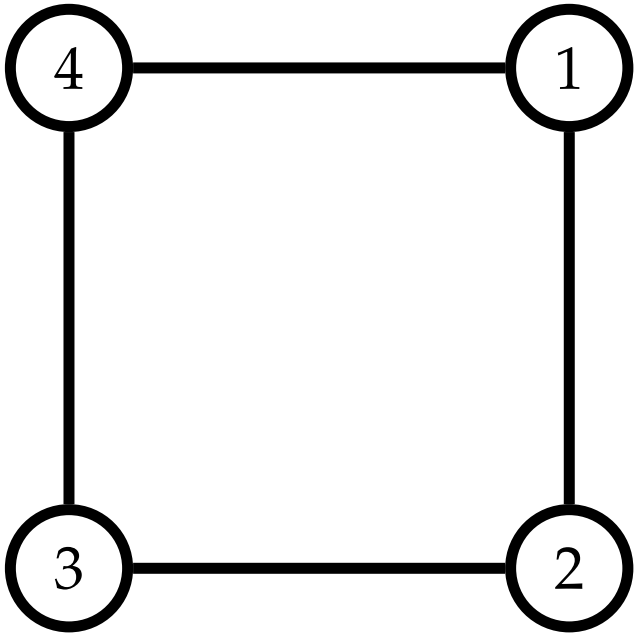
Rotation by 90° clockwise

$$\rho = 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto$$

$$= (1\,2\,3\,4)$$

Reflection in vertical line

$$\sigma = 1 \mapsto 4 \mapsto;\ \ 2 \mapsto 3 \mapsto$$




the dihedral group $D_{\square}$

Rotation by 90° clockwise

$$\rho = 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto$$
$$= (1\,2\,3\,4)$$

Reflection in vertical line

$$\sigma = 1 \mapsto 4 \mapsto;\ \ 2 \mapsto 3 \mapsto$$
$$= (1\,4)(2\,3)$$

The symmetric group $S_n$ the group of all permutations of $n$ points.

The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\ 2), (2\ 3), \ldots, (n\text{-}1\ \ n)$.

The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\ 2), (2\ 3), \ldots, (n\text{-}1\ \ n)$.

**Example** $(\mathbf{1\ 2})(\mathbf{3\ 4\ 5})$

The symmetric group $S_n$ the group of all permutations of $n$ points.

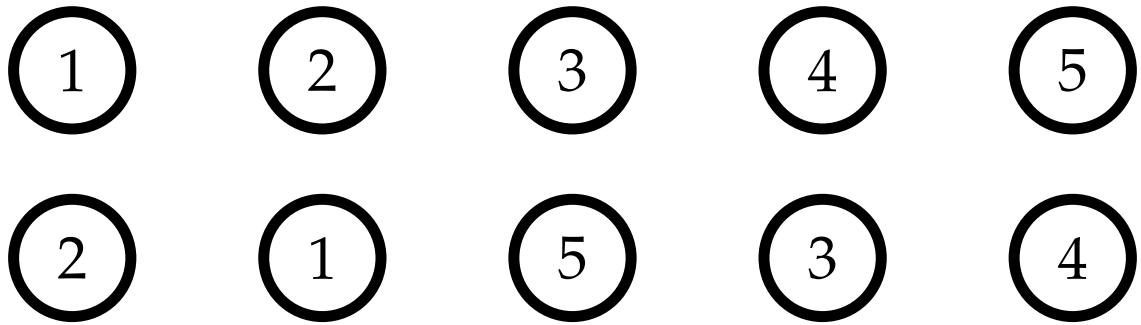
**Fact** $S_n$ is generated by the $n-1$ swaps $(1\ 2), (2\ 3), \ldots, (n\text{-}1\ \ n)$.

**Example** $(\mathbf{1\ 2})(\mathbf{3\ 4\ 5})$

The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\ 2), (2\ 3), \ldots, (n\text{-}1\ \ n)$.

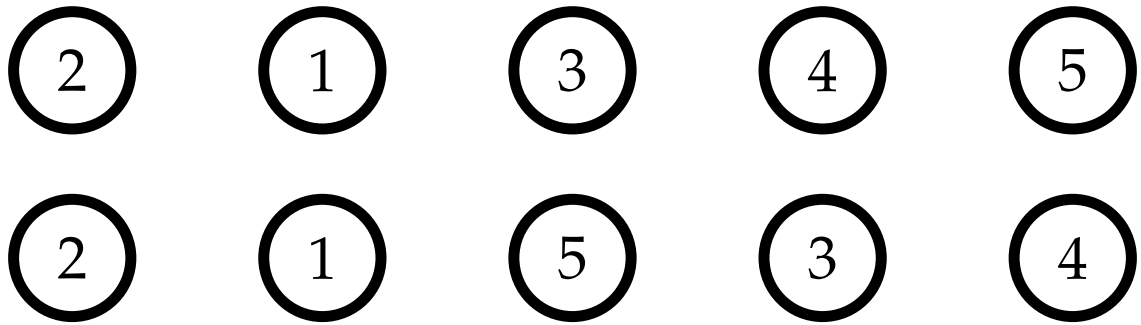
**Example** $(\mathbf{1\ 2})(\mathbf{3\ 4\ 5})$



The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\ 2), (2\ 3), \ldots, (n\text{-}1\ \ n)$.

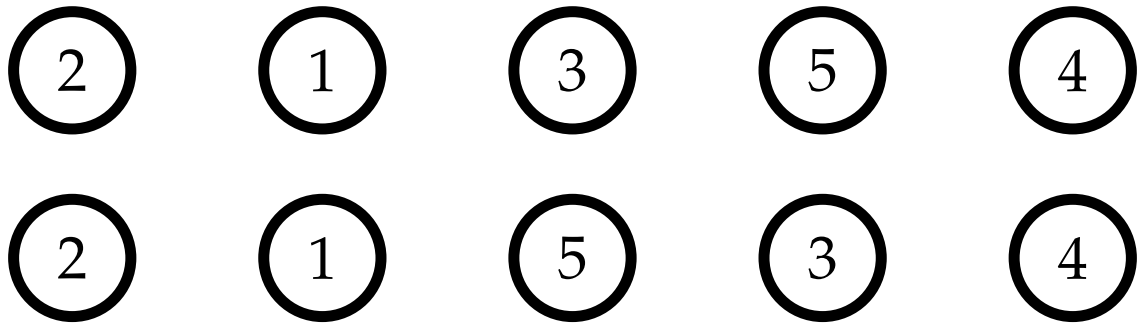
**Example** $(\mathbf{1\ 2})(\mathbf{3\ 4\ 5}) = (\mathbf{1\ 2})$



The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\ 2), (2\ 3), \ldots, (n\text{-}1\ \ n)$.

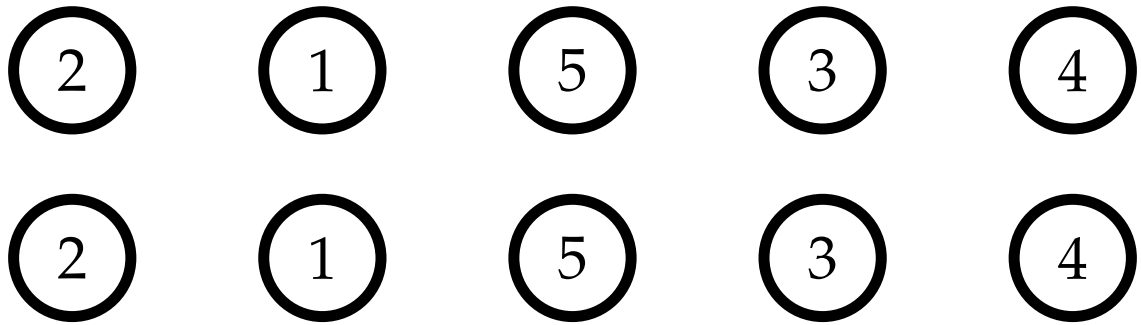
**Example** $(\mathbf{1\ 2})(\mathbf{3\ 4\ 5}) = (\mathbf{1\ 2})(\mathbf{4\ 5})$



The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\ 2), (2\ 3), \ldots, (n\text{-}1\ \ n)$.

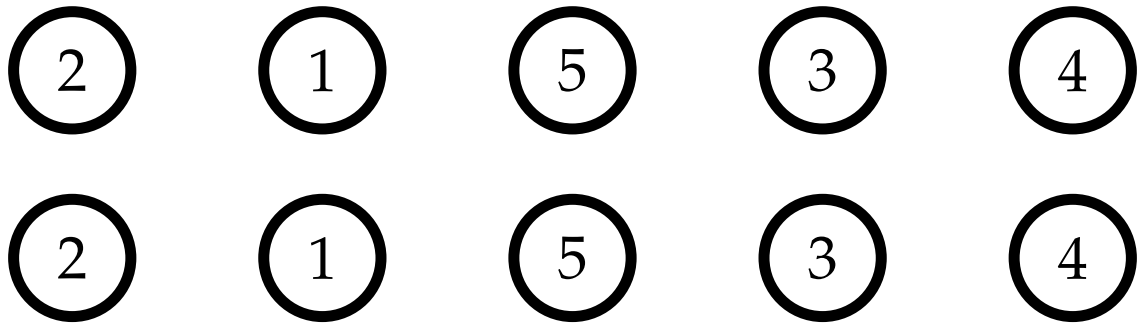
**Example** $(\mathbf{1\ 2})(\mathbf{3\ 4\ 5}) = (\mathbf{1\ 2})(\mathbf{4\ 5})(\mathbf{3\ 5})$



The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\,2), (2\,3), \ldots, (n\text{-}1\ \ n)$.

**Example** $(\mathbf{1\,2})(\mathbf{3\,4\,5}) = (\mathbf{1\,2})(\mathbf{4\,5})(\mathbf{3\,5})$

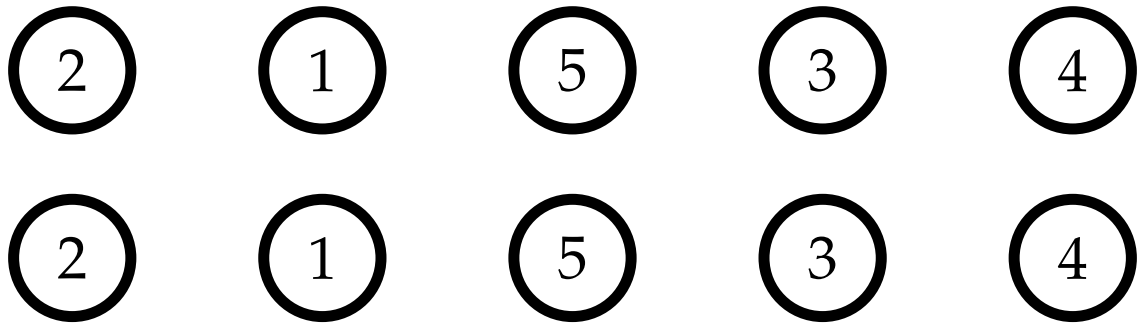



**Fact** $S_n$ is generated by the two permutations $(1\,2)$ and $(1\,2\,\cdots\,n)$.

The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\,2), (2\,3), \ldots, (n\text{-}1\ \ n)$.

**Example** $(\mathbf{1\,2})(\mathbf{3\,4\,5}) = (\mathbf{1\,2})(\mathbf{4\,5})(\mathbf{3\,5})$



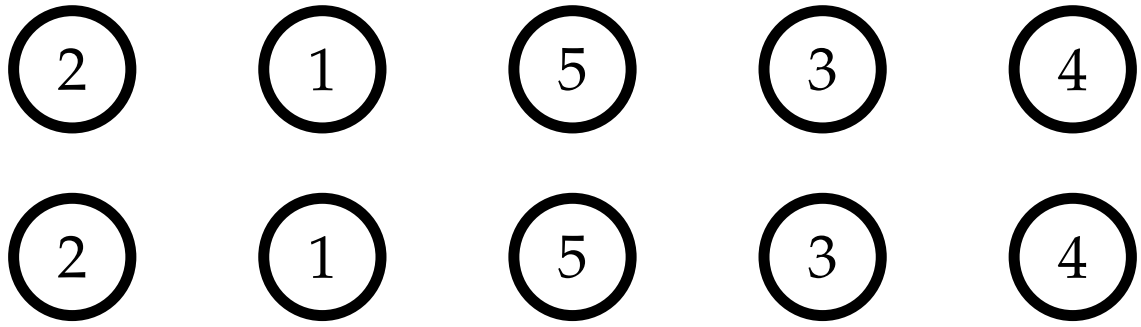

**Fact** $S_n$ is generated by the two permutations $(1\,2)$ and $(1\,2\,\cdots\,n)$.

("Proof": Check that $(1\,2\,\cdots\,n)^{-1}(1\,2)(1\,2\,\cdots\,n) = (2\,3)$.)

The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\ 2), (2\ 3), \ldots, (n\text{-}1\ \ n)$.

**Example** $(\mathbf{1\ 2})(\mathbf{3\ 4\ 5}) = (\mathbf{1\ 2})(\mathbf{4\ 5})(\mathbf{3\ 5})$




**Fact** $S_n$ is generated by the two permutations $(1\ 2)$ and $(1\ 2\ \cdots\ n)$.

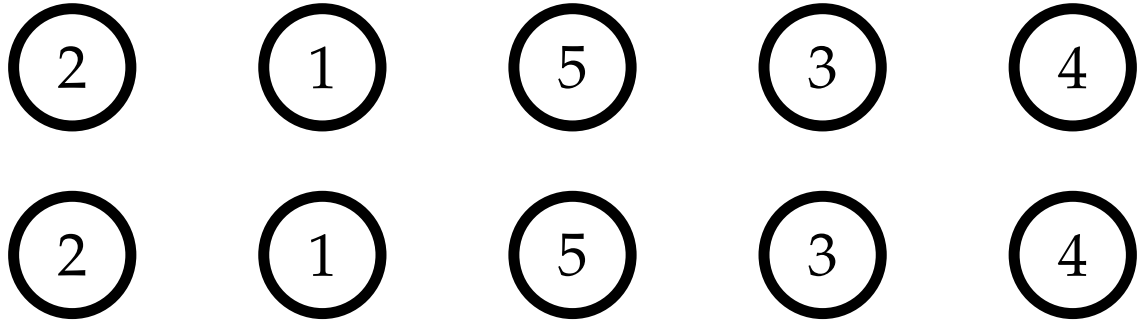
("Proof": Check that $(1\ 2\ \cdots\ n)^{-1}(1\ 2)(1\ 2\ \cdots\ n) = (2\ 3)$.)

The alternating group $A_n$ the group of even permutations of $n$ points.

The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\ 2), (2\ 3), \ldots, (n\text{-}1\ \ n)$.

**Example** $(\mathbf{1\ 2})(\mathbf{3\ 4\ 5}) = (\mathbf{1\ 2})(\mathbf{4\ 5})(\mathbf{3\ 5})$




**Fact** $S_n$ is generated by the two permutations $(1\ 2)$ and $(1\ 2\ \cdots\ n)$.

("Proof": Check that $(1\ 2\ \cdots\ n)^{-1}(1\ 2)(1\ 2\ \cdots\ n) = (2\ 3)$.)

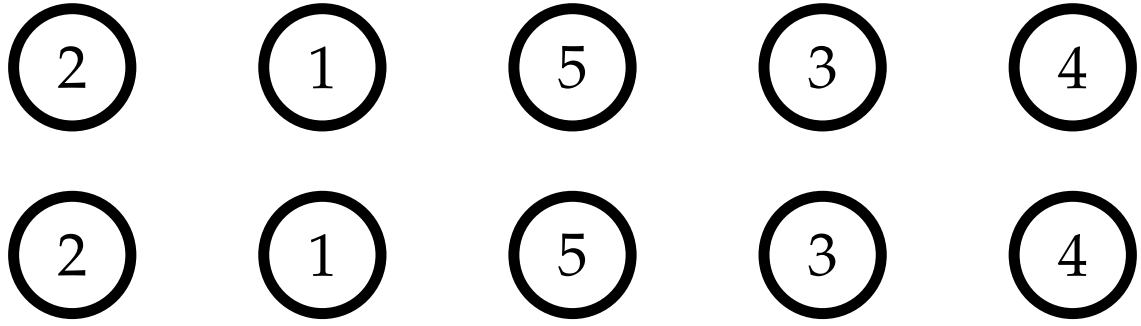
The alternating group $A_n$ the group of even permutations of $n$ points.

**Fact** $A_n$ is generated by two permutations.

The symmetric group $S_n$ the group of all permutations of $n$ points.

**Fact** $S_n$ is generated by the $n-1$ swaps $(1\,2), (2\,3), \ldots, (n\text{-}1\ \ n)$.

**Example** $(\mathbf{1\,2})(\mathbf{3\,4\,5}) = (\mathbf{1\,2})(\mathbf{4\,5})(\mathbf{3\,5})$




**Fact** $S_n$ is generated by the two permutations $(1\,2)$ and $(1\,2\,\cdots\,n)$.

("Proof": Check that $(1\,2\,\cdots\,n)^{-1}(1\,2)(1\,2\,\cdots\,n) = (2\,3)$.)

The alternating group $A_n$ the group of even permutations of $n$ points.

**Fact** $A_n$ is generated by two permutations.

For example, $A_5$ is generated by $(1\,2\,3)$ and $(1\,2\,3\,4\,5)$.

# Generation 1: Galois' Discovery

# Generation 1: Galois' Discovery

Quadratic (Babylonians*) If $ax^2 + bx + c = 0$ with $a \neq 0$ then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

# Generation 1: Galois' Discovery

**Quadratic** (Babylonians*) If $ax^2 + bx + c = 0$ with $a \neq 0$ then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

**Cubic** (Renaissance Italy) If $ax^3 + bx^2 + cx + d = 0$ with $a \neq 0$ then

$$x = \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) + \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}}$$
$$+ \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) - \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} - \frac{b}{3a}$$

**Quartic** Similar to cubic but even more involved!

# Generation 1: Galois' Discovery

**Quadratic** (Babylonians*) If $ax^2 + bx + c = 0$ with $a \neq 0$ then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

**Cubic** (Renaissance Italy) If $ax^3 + bx^2 + cx + d = 0$ with $a \neq 0$ then

$$x = \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) + \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}}$$
$$+ \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) - \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} - \frac{b}{3a}$$

**Quartic** Similar to cubic but even more involved!

**Theorem** (Abel; 1802) There is no formula for the quintic.

How do you factorise a number $a$?

## How do you factorise a number $a$?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \ldots, \quad n_{k-1}/n_k = q_k,$$

and do this so that $q_1, \ldots, q_k$ and $n_k$ are all prime.

## How do you factorise a number $a$?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \ldots, \quad n_{k-1}/n_k = q_k,$$

and do this so that $q_1, \ldots, q_k$ and $n_k$ are all prime.

(A number $p$ is prime if $p$ has exactly two quotients: 1 and $p$.)

## How do you factorise a number $a$?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \ldots, \quad n_{k-1}/n_k = q_k,$$

and do this so that $q_1, \ldots, q_k$ and $n_k$ are all prime.

(A number $p$ is prime if $p$ has exactly two quotients: 1 and $p$.)

## How do you factorise a finite group $G$?

## How do you factorise a number $a$?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \ldots, \quad n_{k-1}/n_k = q_k,$$

and do this so that $q_1, \ldots, q_k$ and $n_k$ are all prime.

(A number $p$ is prime if $p$ has exactly two quotients: 1 and $p$.)

## How do you factorise a finite group $G$?

Repeatedly divide by big normal subgroups:

$$G/N_1 = Q_1, \quad N_1/N_2 = Q_2, \quad \ldots, \quad N_{k-1}/N_k = Q_k,$$

and do this so that $Q_1, \ldots, Q_k$ and $N_k$ are all simple.

## How do you factorise a number $a$?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \ldots, \quad n_{k-1}/n_k = q_k,$$

and do this so that $q_1, \ldots, q_k$ and $n_k$ are all prime.

(A number $p$ is prime if $p$ has exactly two quotients: 1 and $p$.)

## How do you factorise a finite group $G$?

Repeatedly divide by big normal subgroups:

$$G/N_1 = Q_1, \quad N_1/N_2 = Q_2, \quad \ldots, \quad N_{k-1}/N_k = Q_k,$$

and do this so that $Q_1, \ldots, Q_k$ and $N_k$ are all simple.

(A group $S$ is simple if $S$ has exactly two quotients: 1 and $S$.)

**Example** **The symmetry group of a triangle $D_{\triangle}$**

**Example** **The symmetry group of a triangle $D_{\triangle}$**

The subgroup of rotational symmetries $C_3$ is normal in $D_{\triangle}$.

**Example** **The symmetry group of a triangle $D_\triangle$**

The subgroup of rotational symmetries $C_3$ is normal in $D_\triangle$.

Then $D_\triangle / C_3 = C_2$. So the simple factors of $D_\triangle$ are $C_3$ and $C_2$.

**Example** **The symmetry group of a triangle $D_\triangle$**

The subgroup of rotational symmetries $C_3$ is normal in $D_\triangle$.

Then $D_\triangle / C_3 = C_2$. So the simple factors of $D_\triangle$ are $C_3$ and $C_2$.

**Theorem** For a prime $p$, the cyclic group $C_p$ is simple.

**Example** **The symmetry group of a triangle $D_\triangle$**

The subgroup of rotational symmetries $C_3$ is normal in $D_\triangle$.

Then $D_\triangle / C_3 = C_2$. So the simple factors of $D_\triangle$ are $C_3$ and $C_2$.

**Theorem** For a prime $p$, the cyclic group $C_p$ is simple.

**Example** **The symmetric group $S_n$ for $n \geq 5$**

**Example** **The symmetry group of a triangle $D_\triangle$**

The subgroup of rotational symmetries $C_3$ is normal in $D_\triangle$.

Then $D_\triangle / C_3 = C_2$. So the simple factors of $D_\triangle$ are $C_3$ and $C_2$.

**Theorem** For a prime $p$, the cyclic group $C_p$ is simple.

**Example** **The symmetric group $S_n$ for $n \geq 5$**

The subgroup of even permutations $A_n$ is normal in $S_n$.

**Example** **The symmetry group of a triangle $D_\triangle$**

The subgroup of rotational symmetries $C_3$ is normal in $D_\triangle$.

Then $D_\triangle / C_3 = C_2$. So the simple factors of $D_\triangle$ are $C_3$ and $C_2$.

**Theorem** For a prime $p$, the cyclic group $C_p$ is simple.

**Example** **The symmetric group $S_n$ for $n \geq 5$**

The subgroup of even permutations $A_n$ is normal in $S_n$.

Then $S_n / A_n = C_2$. So the simple factors of $S_n$ are $A_n$ and $C_2$.

**Example** **The symmetry group of a triangle $D_\triangle$**

The subgroup of rotational symmetries $C_3$ is normal in $D_\triangle$.

Then $D_\triangle / C_3 = C_2$. So the simple factors of $D_\triangle$ are $C_3$ and $C_2$.

**Theorem** For a prime $p$, the cyclic group $C_p$ is simple.

**Example** **The symmetric group $S_n$ for $n \geq 5$**

The subgroup of even permutations $A_n$ is normal in $S_n$.

Then $S_n / A_n = C_2$. So the simple factors of $S_n$ are $A_n$ and $C_2$.

**Theorem** For $n \geq 5$, the alternating group $A_n$ is simple.

**Theorem** (Galois; 1832) A polynomial is solvable by roots if and only if its symmetry group decomposes into cyclic groups.

**Theorem** (Galois; 1832) A polynomial is solvable by roots if and only if its symmetry group decomposes into cyclic groups.

The equation $x^5 - 5x + 1 = 0$ has symmetry group $S_5$ and so cannot be solved by taking roots.

**Theorem** (Galois; 1832) A polynomial is solvable by roots if and only if its symmetry group decomposes into cyclic groups.

The equation $x^5 - 5x + 1 = 0$ has symmetry group $S_5$ and so cannot be solved by taking roots.

"Please request publicly that Jacobi or Gauss give their opinions, not on the truth but on the importance, of these theorems.

After that I hope people will be found who profit by sorting out all this mess.

I embrace you with affection.

É. GALOIS, 29 May 1832"

# Generation II: Netto's Conjecture

# Generation II: Netto's Conjecture

If we arbitrarily select two or more substitutions of $n$ elements, it is to be regarded as extremely probable that the group of lowest order which contains these is the symmetric group, or at least the alternating group. In the case of two substitutions the probability in favor of the symmetric group may be taken as about $\frac{3}{4}$, and in favor of the alternating, but not symmetric, group as about $\frac{1}{4}$. In order that any given substitutions may generate a group which is only a part of the $n!$ possible substitutions, very special relations are necessary, and it is highly improbable that arbitrarily chosen substitutions $s_i = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix}$ should satisfy these conditions. The exception most likely to occur would be that all the given substitutions were severally equivalent to an even number of transpositions and would consequently generate the alternating group.

E. Netto, *The theory of substitutions and its application to algebra*, Trans. F. N. Cole, Ann Arbor, Michigan, (1892)

Let $P(G)$ be the probability that two random elements generate $G$.

**Netto's Conjecture** $P(A_n) \to 1$ as $n \to \infty$.

Let $P(G)$ be the probability that two random elements generate $G$.

**Netto's Conjecture** $P(A_n) \to 1$ as $n \to \infty$.

## Cyclic groups of prime order

Let $p$ be prime. Then

$$P(C_p) = \frac{p^2 - 1}{p^2}$$

and so $P(C_p) \to 1$ as $p \to \infty$.

Let $P(G)$ be the probability that two random elements generate $G$.

**Netto's Conjecture** $P(A_n) \to 1$ as $n \to \infty$.

## Cyclic groups of prime order

Let $p$ be prime. Then

$$P(C_p) = \frac{p^2 - 1}{p^2}$$

and so $P(C_p) \to 1$ as $p \to \infty$.

## Numerical evidence

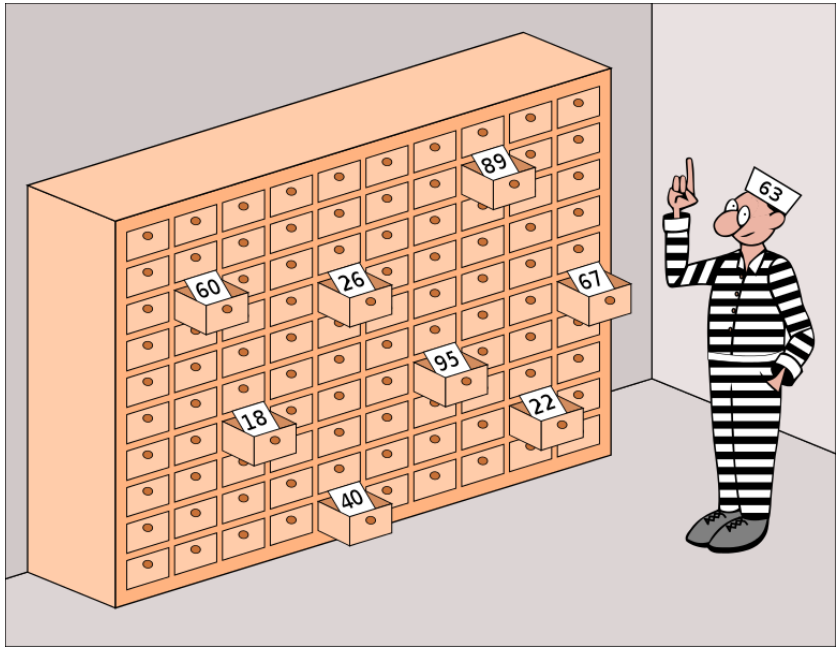
| $n$ | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|
| $P(A_n)$ | 0.633 | 0.588 | 0.726 | 0.738 | 0.848 | 0.875 |

GAP computations by N. Menezes, M. Quick and C. M. Roney-Dougal

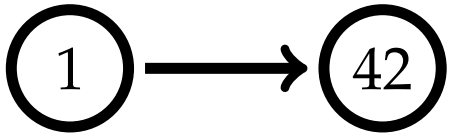
# Generation III: Dixon's Conjecture

# Generation III: Dixon's Conjecture

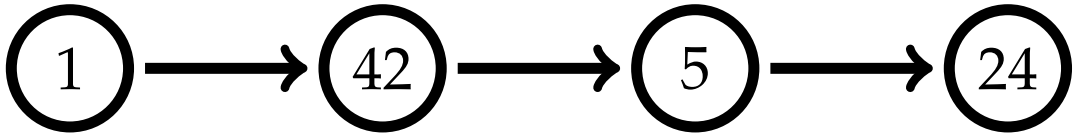
A final chance is given to 100 prisoners, numbered 1 to 100. A room contains 100 closed drawers which contain the numbers 1 to 100. One by one, the prisoners enter the room and choose 50 drawers to open. The drawers are closed again. If every prisoner finds his number, all prisoners are pardoned. However, if just one prisoner does not find his number, all prisoners remain imprisoned. Before any prisoner enters the room, they may decide on a strategy but they may not communicate once the first prisoner enters. What is the best strategy?

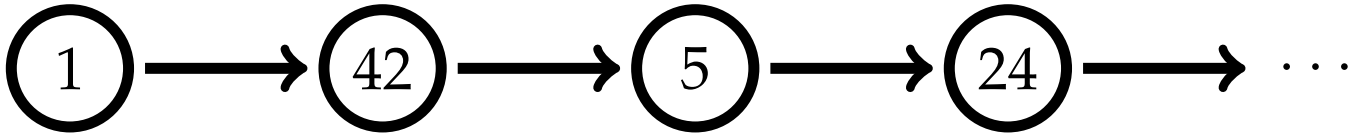


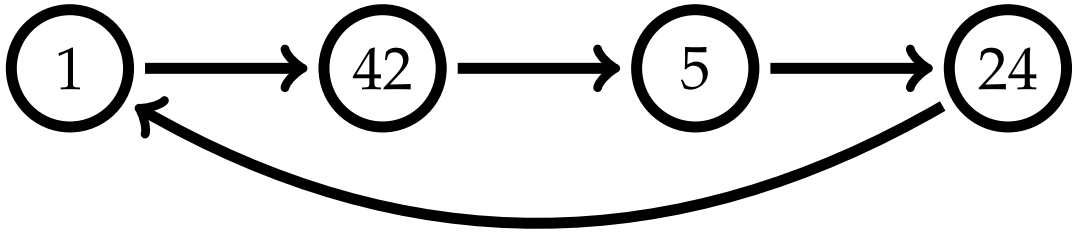

1

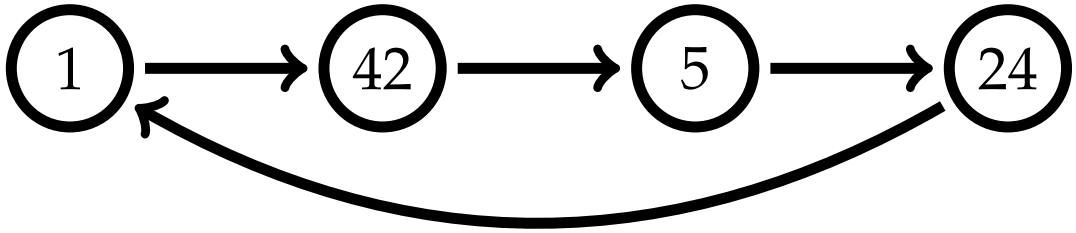

1
42


1
42
5

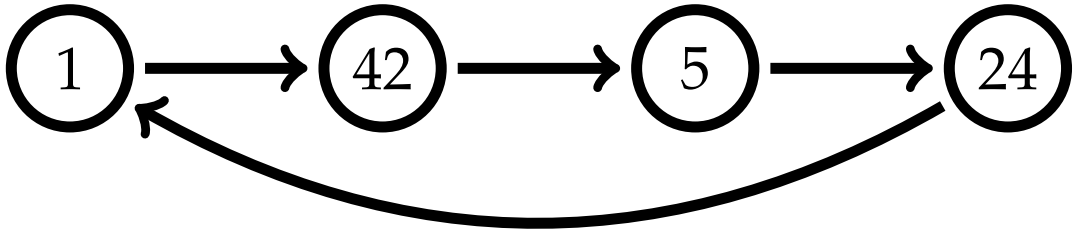

1
42
5
24


1
42
5
24
· · ·


1
42
5
24

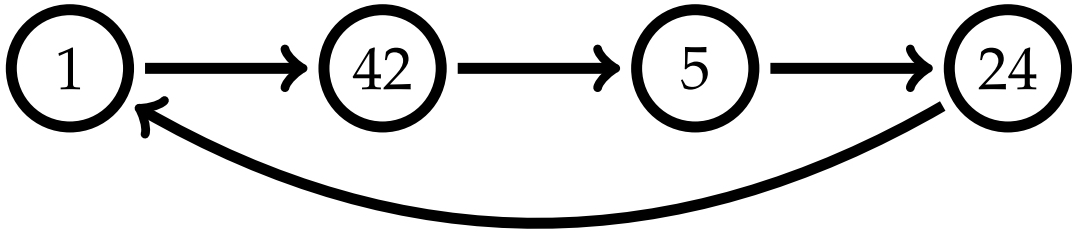



All prisoners succeed if there is no cycle of length longer than 50.




All prisoners succeed if there is no cycle of length longer than 50.

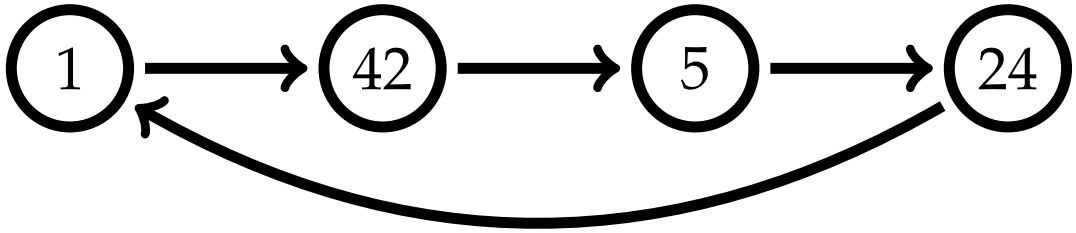
How likely is this?




All prisoners succeed if there is no cycle of length longer than 50.

How likely is this?

**Exercise** For $\ell > n$, the probability that a permutation of $2n$ points has a cycle of length $\ell$ is $1/\ell$.




All prisoners succeed if there is no cycle of length longer than 50.

How likely is this?

**Exercise** For $\ell > n$, the probability that a permutation of $2n$ points has a cycle of length $\ell$ is $1/\ell$.

The probability that a permutation of 100 points has no cycle of length longer than 50 is

$$1 - \left( \frac{1}{51} + \frac{1}{52} + \cdots + \frac{1}{100} \right) \approx 0.312$$

which is the probability of success.

Between 1965 and 1968, Paul Erdős and Pál Turán published several papers on random permutations and this was the birth of the field of probabilistic group theory.

Between 1965 and 1968, Paul Erdős and Pál Turán published several papers on random permutations and this was the birth of the field of probabilistic group theory.

In 1969, John Dixon was reading Netto's book and came across his conjecture. Using the work of Erdős and Turán he proved it.

**Theorem** $P(A_n) \to 1$ as $n \to \infty$.

Between 1965 and 1968, Paul Erdős and Pál Turán published several papers on random permutations and this was the birth of the field of probabilistic group theory.

In 1969, John Dixon was reading Netto's book and came across his conjecture. Using the work of Erdős and Turán he proved it.

**Theorem** $P(A_n) \to 1$ as $n \to \infty$.

Dixon replaced one conjecture with another even bolder one.

Between 1965 and 1968, Paul Erdős and Pál Turán published several papers on random permutations and this was the birth of the field of probabilistic group theory.

In 1969, John Dixon was reading Netto's book and came across his conjecture. Using the work of Erdős and Turán he proved it.

**Theorem** $P(A_n) \to 1$ as $n \to \infty$.

Dixon replaced one conjecture with another even bolder one.

**Dixon's Conjecture** For simple groups $G$, $P(G) \to 1$ as $|G| \to \infty$.

Between 1965 and 1968, Paul Erdős and Pál Turán published several papers on random permutations and this was the birth of the field of probabilistic group theory.

In 1969, John Dixon was reading Netto's book and came across his conjecture. Using the work of Erdős and Turán he proved it.

**Theorem** $P(A_n) \to 1$ as $n \to \infty$.

Dixon replaced one conjecture with another even bolder one.

**Dixon's Conjecture** For simple groups $G$, $P(G) \to 1$ as $|G| \to \infty$.

That all the known finite simple groups could be generated by two elements was only proved in 1962.

Between 1965 and 1968, Paul Erdős and Pál Turán published several papers on random permutations and this was the birth of the field of probabilistic group theory.

In 1969, John Dixon was reading Netto's book and came across his conjecture. Using the work of Erdős and Turán he proved it.

**Theorem** $P(A_n) \to 1$ as $n \to \infty$.

Dixon replaced one conjecture with another even bolder one.

**Dixon's Conjecture** For simple groups $G$, $P(G) \to 1$ as $|G| \to \infty$.

That all the known finite simple groups could be generated by two elements was only proved in 1962.

What if there were other finite simple groups?

# Generation IV: An Enormous Theorem

Which finite groups are simple?

# Generation IV: An Enormous Theorem

Which finite groups are simple?

- cyclic groups of prime order

# Generation IV: An Enormous Theorem

Which finite groups are simple?

- cyclic groups of prime order
- alternating groups of degree at least 5

# Generation IV: An Enormous Theorem

Which finite groups are simple?

- cyclic groups of prime order
- alternating groups of degree at least 5
- groups of Lie type

# Generation IV: An Enormous Theorem

Which finite groups are simple?

- cyclic groups of prime order
- alternating groups of degree at least 5
- groups of Lie type (e.g. $\mathrm{SL}_2(\mathbb{F}_p)$)

# Generation IV: An Enormous Theorem

Which finite groups are simple?

- cyclic groups of prime order
- alternating groups of degree at least 5
- groups of Lie type (e.g. $\mathrm{SL}_2(\mathbb{F}_p)$)
- five sporadic Mathieu groups

# Generation IV: An Enormous Theorem

Which finite groups are simple?

- cyclic groups of prime order
- alternating groups of degree at least 5
- groups of Lie type (e.g. $\mathrm{SL}_2(\mathbb{F}_p)$)
- five sporadic Mathieu groups

Are there any more?

# Generation IV: An Enormous Theorem

Which finite groups are simple?

- cyclic groups of prime order
- alternating groups of degree at least 5
- groups of Lie type (e.g. $\mathrm{SL}_2(\mathbb{F}_p)$)
- five sporadic Mathieu groups

Are there any more?

1954 Brauer calls mathematicians to classify the finite simple groups

# Generation IV: An Enormous Theorem

Which finite groups are simple?

- cyclic groups of prime order
- alternating groups of degree at least 5
- groups of Lie type (e.g. $\mathrm{SL}_2(\mathbb{F}_p)$)
- five sporadic Mathieu groups

Are there any more?

1954 Brauer calls mathematicians to classify the finite simple groups

1963 Feit and Thompson take 250 pages to prove that every non-cyclic finite simple group has even order

# Generation IV: An Enormous Theorem

Which finite groups are simple?

- cyclic groups of prime order
- alternating groups of degree at least 5
- groups of Lie type (e.g. $\mathrm{SL}_2(\mathbb{F}_p)$)
- five sporadic Mathieu groups

Are there any more?

1954 Brauer calls mathematicians to classify the finite simple groups

1963 Feit and Thompson take 250 pages to prove that every non-cyclic finite simple group has even order

1965 Janko finds three more sporadic groups

# A Simple Ballad

What are the orders of all simple groups?
I speak of the honest ones, not of the loops.
It seems that old Burnside their orders has guessed:
Except of the cyclic ones, even the rest.

Groups made up of permutes will produce more:
For $A_n$ is simple, if $n$ exceeds 4.
Then, there was Sir Matthew who came into view
Exhibiting groups of an order quite new.

Still others have come on to study this thing.
Of Artin and Chevalley now we shall sing.
With matrices finite they made quite a list.
The question is: Could there be others they've missed?

Suzuki and Ree then maintained it's the case
These methods had not reached the end of the chase.
They wrote down some matrices, just four by four,
that made up a simple group. Why not make more?

And then came up the opus of Thompson and Feit
Which shed on the problem remarkable light.
A group, when the order won't factor by two,
Is cyclic or solvable. That's what true.

Suzuki and Ree had caused eyebrows to raise,
But the theoreticians they just couldn't face.
Their groups were not new: if you added a twist,
You'd get them from old ones with a flick of the wrist.

Still, some hardy souls felt a thorn in their side.
For the five groups of Mathieu all reason defied:
Not $A_n$, not twisted, and not Chevalley.
They called them sporadic and filed them away.

Are Mathieu groups creatures of heaven or hell?
Zvonimir Janko determined to tell.
He found out what nobody wanted to know:
The masters had missed 1 7 5 5 6 0.

The floodgates were open! New groups were the rage!
(And twelve or more sprouted, to greet the new age.)
By Janko and Conway and Fischer and Held,
McLaughlin, Suzuki, and Higman, and Sims.

No doubt you noted the last lines don't rhyme.
Well, that is, quite simply, a sign of the time.
There's chaos, not order, among simple groups,
And maybe we'd better go back to the loops.

1972 Gorenstein provides a “16-step plan”

1972 Gorenstein provides a “16-step plan”

1975 Janko finds the 26th (and final) sporadic group

1972 Gorenstein provides a “16-step plan”

1975 Janko finds the 26th (and final) sporadic group

1980 Greiss constructs the Monster whose is order is

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

1972 Gorenstein provides a “16-step plan”

1975 Janko finds the 26th (and final) sporadic group

1980 Greiss constructs the Monster whose is order is

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

1983 The Classification is completed

1972 Gorenstein provides a “16-step plan”

1975 Janko finds the 26th (and final) sporadic group

1980 Greiss constructs the Monster whose is order is

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

1983 The Classification is completed

2004 The Classification is actually completed

1972 Gorenstein provides a "16-step plan"

1975 Janko finds the 26th (and final) sporadic group

1980 Greiss constructs the Monster whose is order is

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

1983 The Classification is completed

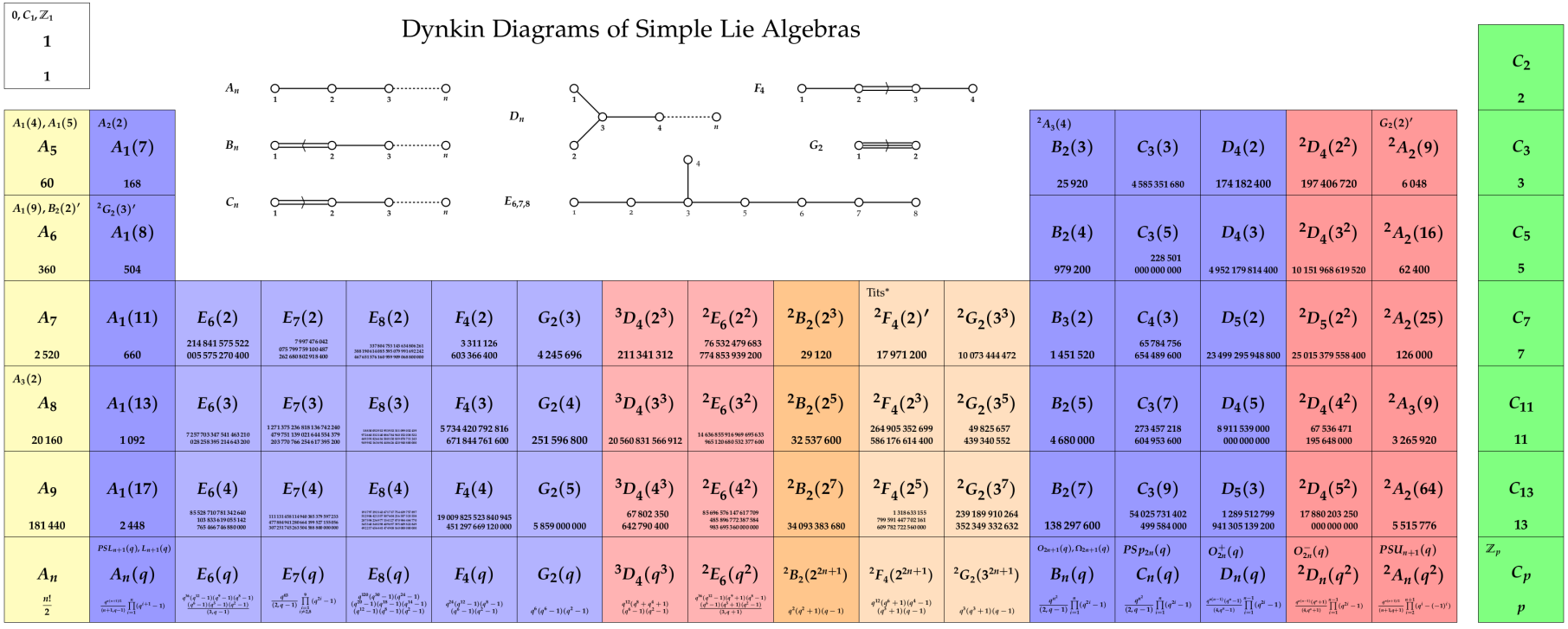
2004 The Classification is actually completed

**Theorem** (The Classification of Finite Simple Groups)

Any finite simple group is isomorphic to one of the following

- a cyclic group of prime order
- an alternating group of degree at least five
- a group of Lie type
- one of 26 sporadic groups

# The Periodic Table Of Finite Simple Groups




https://irandrus.files.wordpress.com/2012/06/periodic-table-of-groups.pdf

# Consequences of the Classification

## Consequences of the Classification

The theorem of Steinberg (1962) together with the proof for the sporadic groups gives the following.

**Theorem** Every finite simple group is generated by two elements.

## Consequences of the Classification

The theorem of Steinberg (1962) together with the proof for the sporadic groups gives the following.

**Theorem** Every finite simple group is generated by two elements.

Theorems of Kantor & Lubotzky (1990) and Liebeck & Shalev (1995) proves Dixon's conjecture.

**Theorem** For simple groups $G$, $P(G) \to 1$ as $|G| \to \infty$.

## Consequences of the Classification

The theorem of Steinberg (1962) together with the proof for the sporadic groups gives the following.

**Theorem** Every finite simple group is generated by two elements.

Theorems of Kantor & Lubotzky (1990) and Liebeck & Shalev (1995) proves Dixon's conjecture.

**Theorem** For simple groups $G$, $P(G) \to 1$ as $|G| \to \infty$.

A theorem of Menezes, Quick and Roney-Dougal (2013)

**Theorem** For simple groups $G$, $P(G) \geq \frac{53}{90}$.

# Generation V: Our Generation(’s) Work

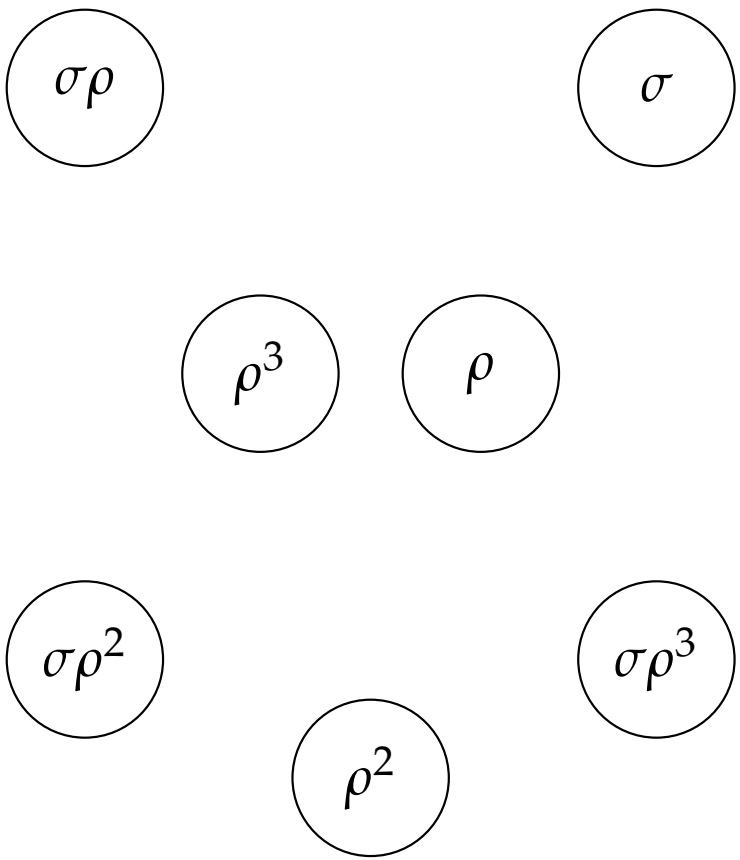
# Generation V: Our Generation(’s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

# Generation V: Our Generation('s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

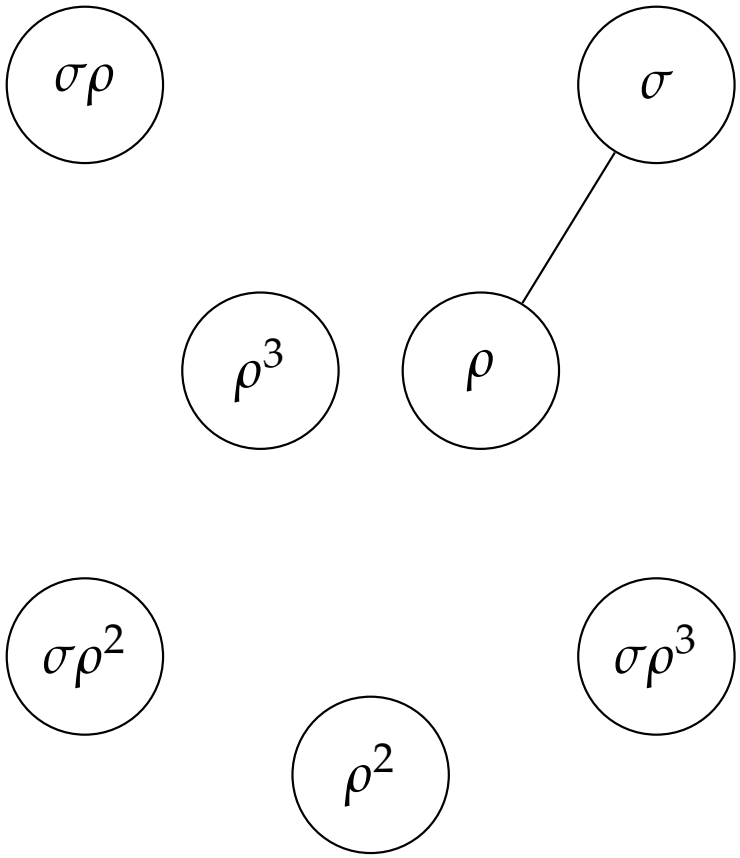
Dihedral group $D_{\square}$



# Generation V: Our Generation('s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

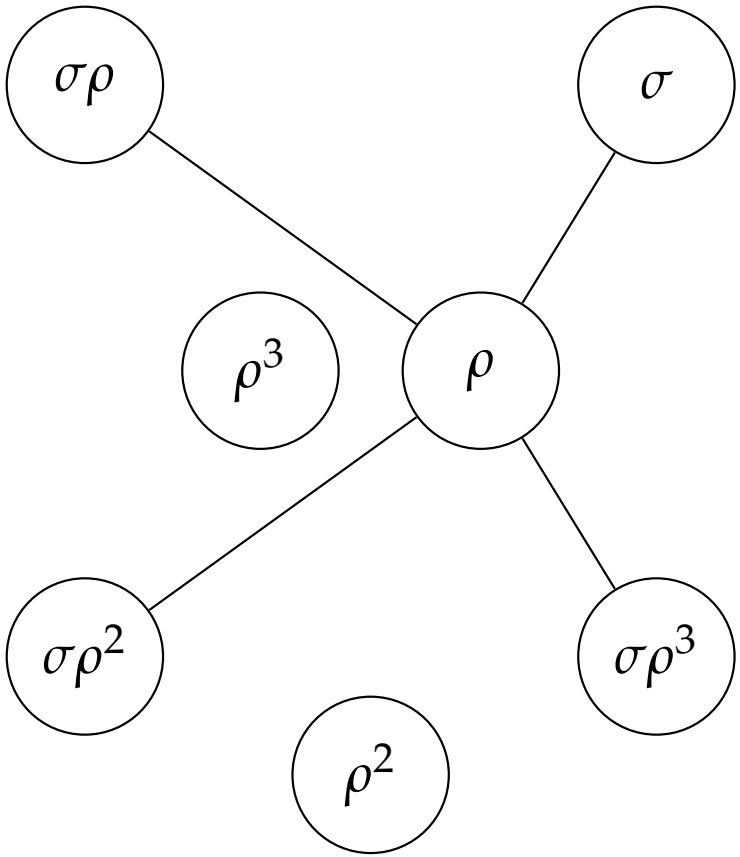
Dihedral group $D_{\square}$



# Generation V: Our Generation('s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

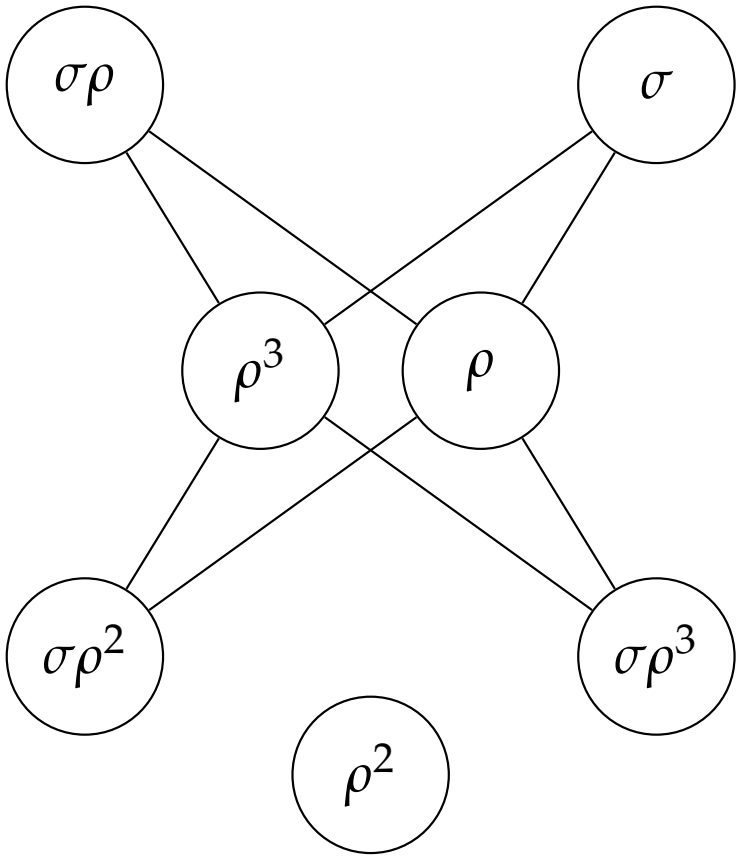
Dihedral group $D_{\square}$



# Generation V: Our Generation('s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

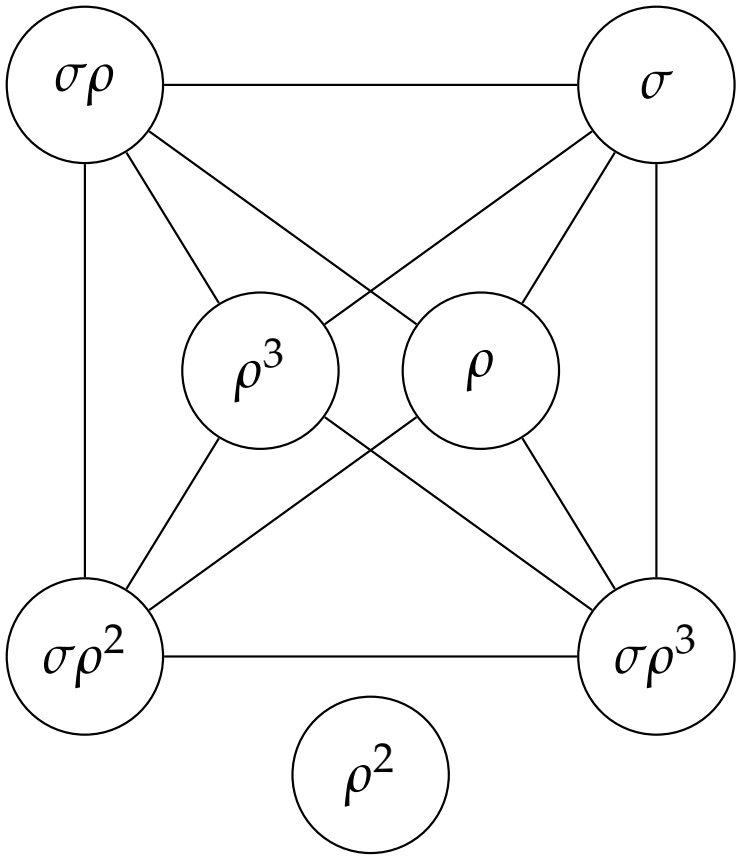
Dihedral group $D_{\square}$



# Generation V: Our Generation(’s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

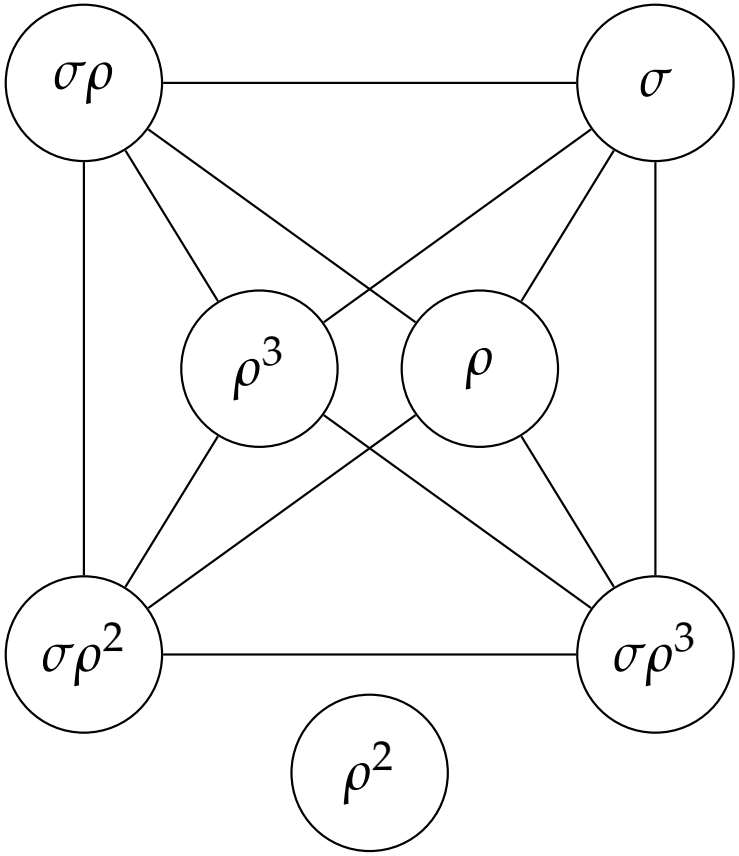
Dihedral group $D_{\square}$



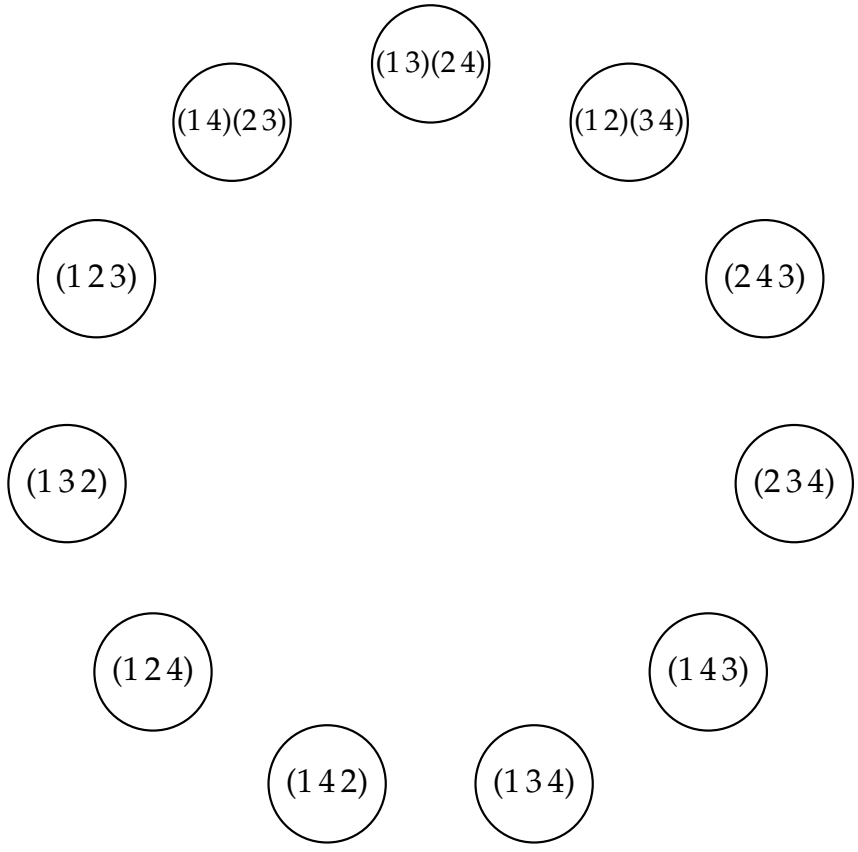
# Generation V: Our Generation(’s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

## Dihedral group $D_{\square}$



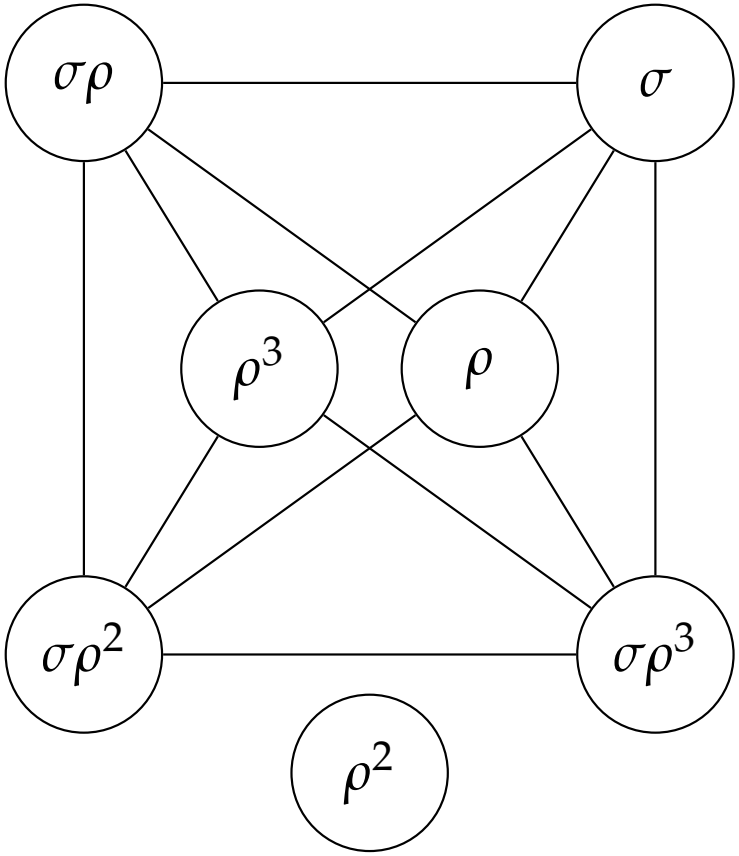

## Alternating group $A_4$



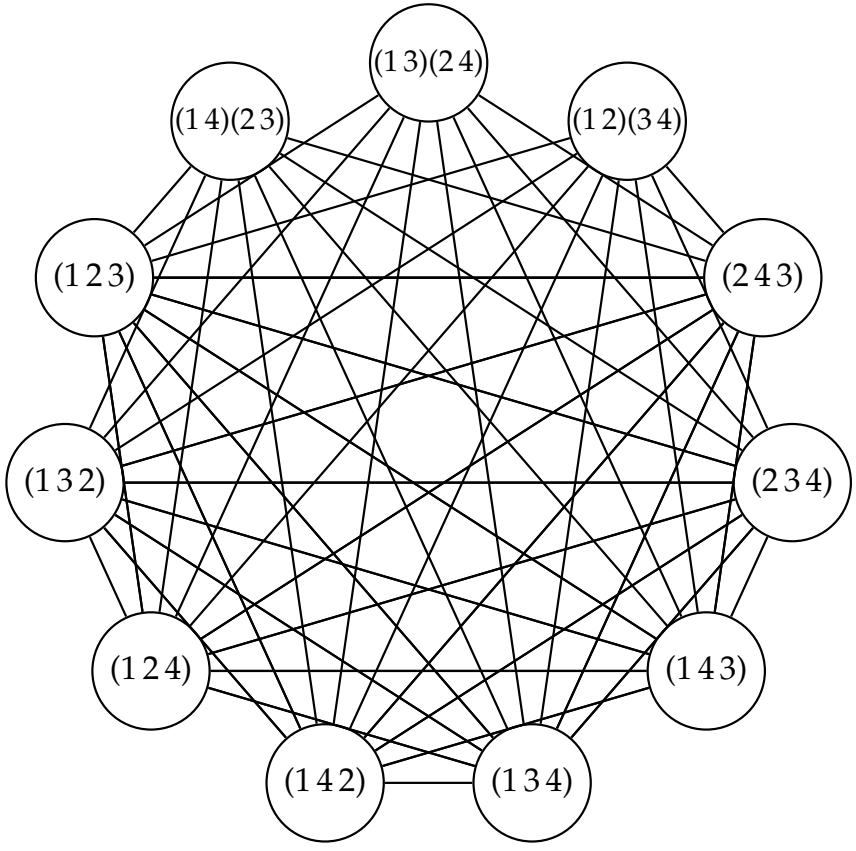
# Generation V: Our Generation(’s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group $D_{\square}$



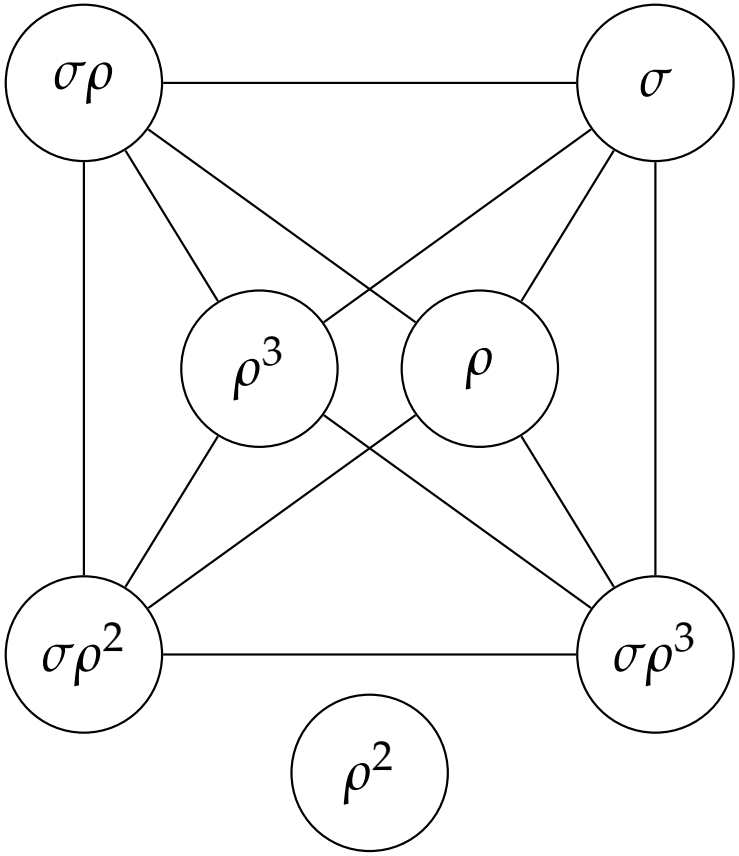

Alternating group $A_4$



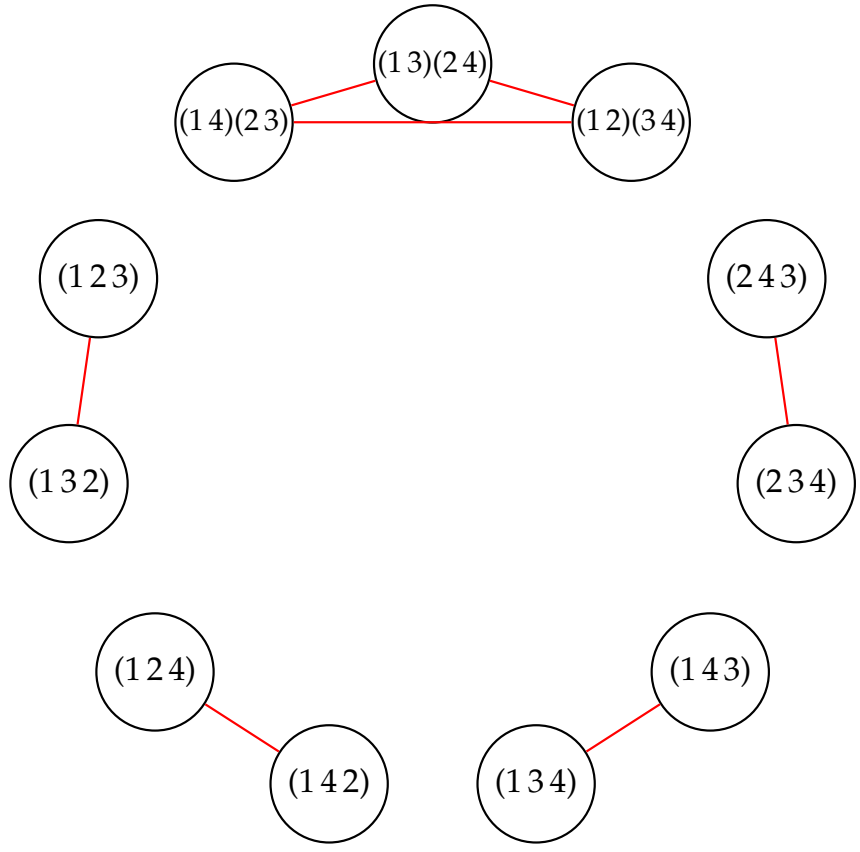
# Generation V: Our Generation('s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

## Dihedral group $D_{\square}$



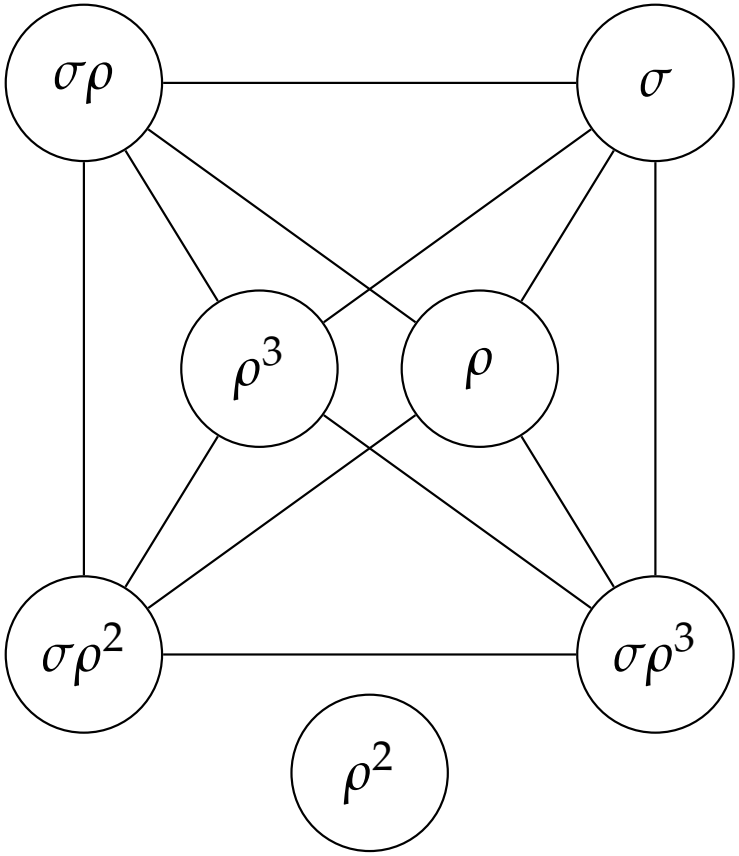

## Alternating group $A_4$



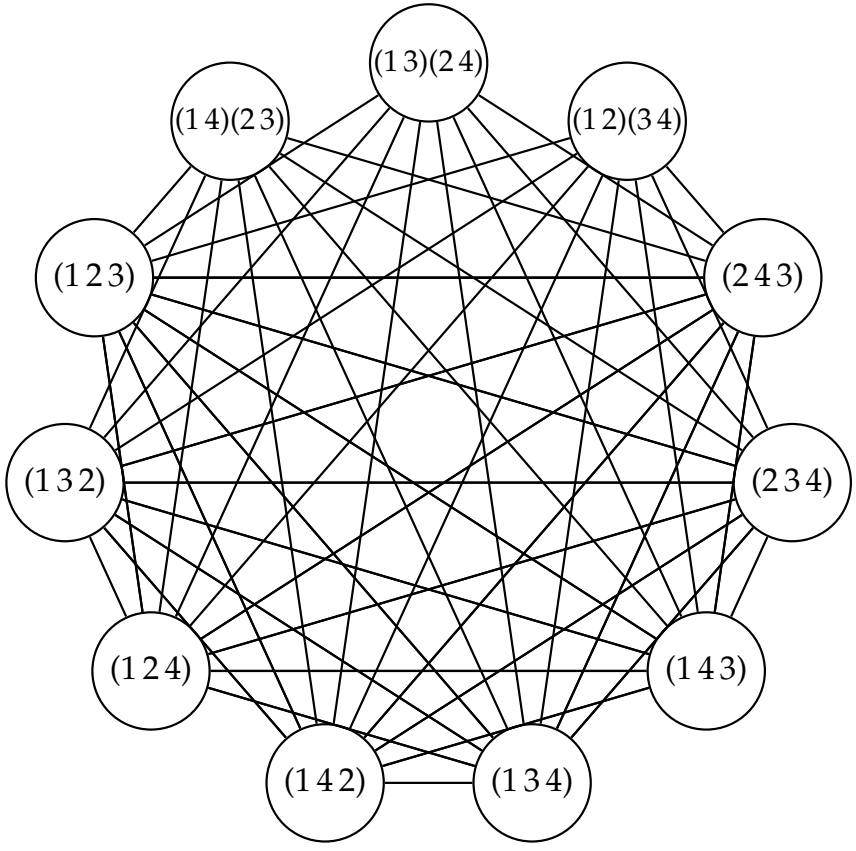
# Generation V: Our Generation(’s) Work

Consider the graph whose vertices are the non-identity elements of $G$ such that two vertices $g$ and $h$ are adjacent if and only if $\langle g, h \rangle = G$.

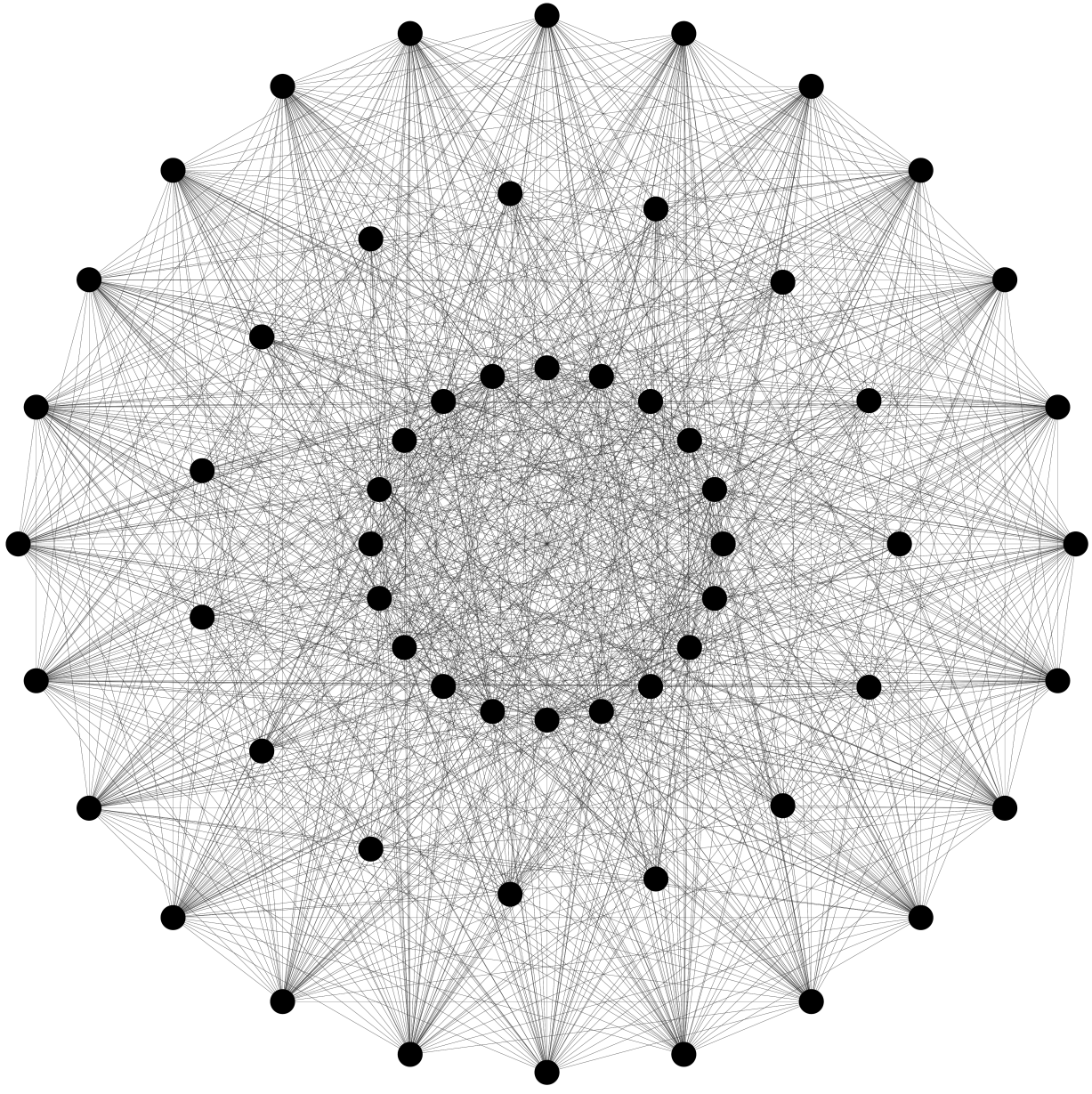
Dihedral group $D_{\square}$




Alternating group $A_4$



# Alternating group $A_5$



**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

Which other finite groups have this property?

**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

Which other finite groups have this property?

**Proposition** If every non-identity element is contained in a generating pair then every quotient is cyclic.

**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

Which other finite groups have this property?

**Proposition** If every non-identity element is contained in a generating pair then every quotient is cyclic.

**Proof**

**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

Which other finite groups have this property?

**Proposition** If every non-identity element is contained in a generating pair then every quotient is cyclic.

**Proof** Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$.

**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

Which other finite groups have this property?

**Proposition** If every non-identity element is contained in a generating pair then every quotient is cyclic.

**Proof** Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. By assumption, $\langle x, n \rangle = G$ for some $x \in G$.

**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

Which other finite groups have this property?

**Proposition** If every non-identity element is contained in a generating pair then every quotient is cyclic.

**Proof** Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. By assumption, $\langle x, n \rangle = G$ for some $x \in G$. In particular, $\langle xN, nN \rangle = G/N$.

**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

Which other finite groups have this property?

**Proposition** If every non-identity element is contained in a generating pair then every quotient is cyclic.

**Proof** Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. By assumption, $\langle x, n \rangle = G$ for some $x \in G$. In particular, $\langle xN, nN \rangle = G/N$. Since $nN$ is trivial in the quotient $G/N$, in fact, $G/N = \langle xN \rangle$.

**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

Which other finite groups have this property?

**Proposition** If every non-identity element is contained in a generating pair then every quotient is cyclic.

**Proof** Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. By assumption, $\langle x, n \rangle = G$ for some $x \in G$. In particular, $\langle xN, nN \rangle = G/N$. Since $nN$ is trivial in the quotient $G/N$, in fact, $G/N = \langle xN \rangle$. So $G/N$ is cyclic. $\square$

**Theorem** (Guralnick & Kantor, 2000) If $G$ is a finite simple group then every non-identity element of $G$ is contained in a generating pair.

Which other finite groups have this property?

**Proposition** If every non-identity element is contained in a generating pair then every quotient is cyclic.

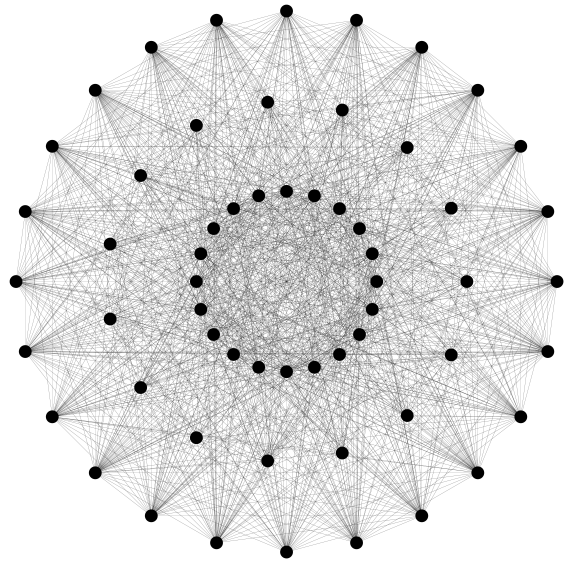
**Proof** Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. By assumption, $\langle x, n \rangle = G$ for some $x \in G$. In particular, $\langle xN, nN \rangle = G/N$. Since $nN$ is trivial in the quotient $G/N$, in fact, $G/N = \langle xN \rangle$. So $G/N$ is cyclic. □

**Conjecture** For finite groups, every non-identity element is contained in a generating pair if and only if every proper quotient is cyclic.

# Group Generation Through the Generations

Scott Harper

University of Bristol



St Andrews University Mathematics Society

3rd March 2017