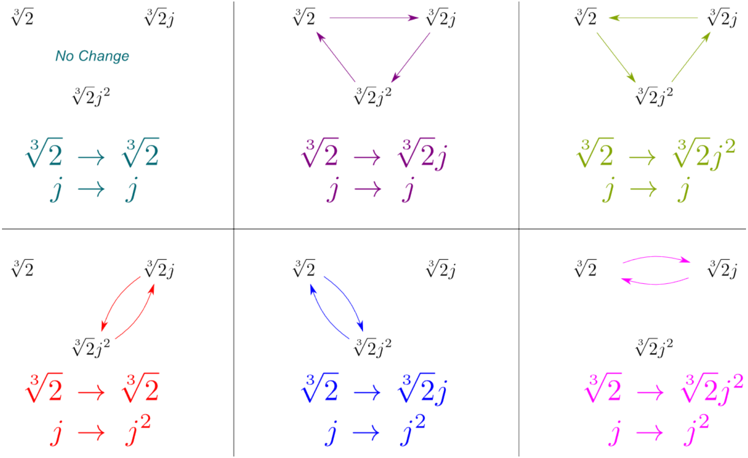
What are...the groups of Galois theory?

Or: An ocean of symmetric groups

Symmetries of roots

S_3 acts on roots$(x^3 - 2)$:



- **Galois group $G(f)$** = symmetry group of roots of a polynomial $f \in \mathbb{Q}[x]$
- **Example** $G(x^3 - 2)$ is S_3
- **Open question** Do all finite groups appear as $G(f)$ for some f?

Small = easy

$G(x^5 - x - 1) = S_5$:

```
In[2]:= Roots[x^5 - x - 1 == 0, x]
Out[2]= x == 1.17… || x == -0.765… - 0.352… i ||
        x == -0.765… + 0.352… i ||
        x == 0.181… - 1.08… i || x == 0.181… + 1.08… i
```

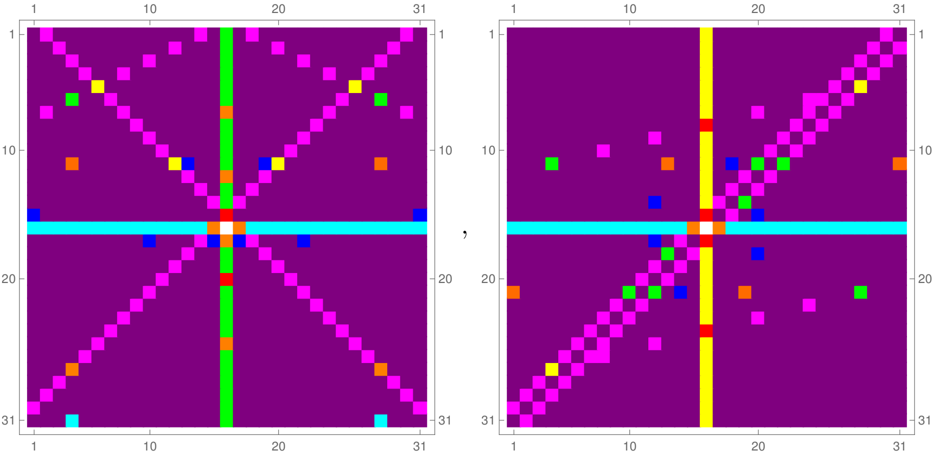
$G(x^5 + x - 1) = D_6$:

In[3]:= `Roots[x^5 + x - 1 == 0, x]`

Out[3]= $x == \frac{1}{3}\left(-1 + \left(\frac{25}{2} - \frac{3\sqrt{69}}{2}\right)^{1/3} + \left(\frac{1}{2}\left(25 + 3\sqrt{69}\right)\right)^{1/3}\right) \mid\mid x ==$
$-\frac{1}{3} - \frac{1}{6}\left(1 + i\sqrt{3}\right)\left(\frac{25}{2} - \frac{3\sqrt{69}}{2}\right)^{1/3} - \frac{1}{6}\left(1 - i\sqrt{3}\right)\left(\frac{1}{2}\left(25 + 3\sqrt{69}\right)\right)^{1/3} \mid\mid$
$x == -\frac{1}{3} - \frac{1}{6}\left(1 - i\sqrt{3}\right)\left(\frac{25}{2} - \frac{3\sqrt{69}}{2}\right)^{1/3} -$
$\frac{1}{6}\left(1 + i\sqrt{3}\right)\left(\frac{1}{2}\left(25 + 3\sqrt{69}\right)\right)^{1/3} \mid\mid x == (-1)^{1/3} \mid\mid x == -(-1)^{2/3}$

- $G(f)$ **measures** how difficult it is to express the roots of f (solvability)
- **Example** $G(f) = S_5$ and roots are "random" ⇝ no easy formula; $G(f) = D_6$ and roots are iterated radicals
- **Question** How difficult is it to express roots?

An ocean of symmetric groups



- Worst case for f of degree five is S_5
- Plots above Left: $G(x^5+ax+b)$; right $G(x^5+ax^2+b)$; for $a, b \in \{-15, \ldots, 15\}$
- Color code for $\#G(f)$ $1 \rightarrow$ White, $2 \rightarrow$ Red, $4 \rightarrow$ Orange, $6 \rightarrow$ Yellow, $8 \rightarrow$ Green, $12 \rightarrow$ Blue, $20 \rightarrow$ Cyan, $24 \rightarrow$ Magenta, $120 \rightarrow$ Purple

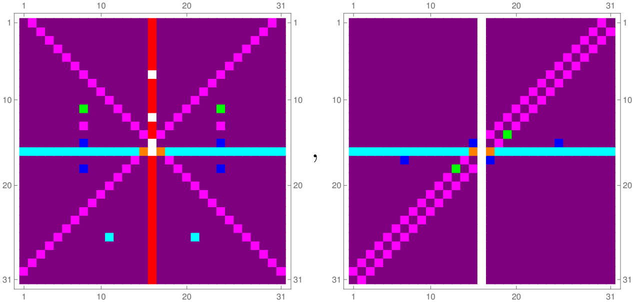
Enter, the theorem

Let $All(N) = \{f \in \mathbb{Z}[x] | \deg f = n, \sum |coeffs(f)| < N\}$ and
$S_n(N) = \{f \in \mathbb{Z}[x] | \deg f = n, \sum |coeffs(f)| < N, G(f) = S_n\}$

$$\lim_{N\to\infty} \#S_n(N)/\#All(N) \to 1$$

Essentially all Galois groups are symmetric groups

- Essentially all polynomials have "random" roots
- Here are $G(x^5+ax^3+b)$ and $G(x^5+ax^4+b)$ for completeness:



Radicals of radicals of...

$G(x^5-15x-14) = S_4$:

```
In[1]:= a := -15;
        b := -14;
        Roots[x^5 + a * x + b == 0, x]
```

Out[3]=

$$x == \frac{1}{4} - \frac{1}{4\sqrt{\frac{3}{-5-\frac{136\cdot 5^{2/3}}{\left(65+3\sqrt{22305}\right)^{1/3}}+4\left(5\cdot\left(65+3\sqrt{22305}\right)\right)^{1/3}}}} - \frac{1}{2}\cdot\sqrt{\left(-\frac{5}{6}+\frac{34\cdot 5^{2/3}}{3\left(65+3\sqrt{22305}\right)^{1/3}}-\frac{1}{3}\left(5\cdot\left(65+3\sqrt{22305}\right)\right)^{1/3} - \frac{5}{2}\sqrt{\frac{3}{-5-\frac{136\cdot 5^{2/3}}{\left(65+3\sqrt{22305}\right)^{1/3}}+4\left(5\cdot\left(65+3\sqrt{22305}\right)\right)^{1/3}}}\right)} \;||$$

- The first not solvable group is A_5
- For all smaller groups one gets radical expressions
- However, these radical expressions are slightly obscure

Thank you for your attention!

I hope that was of some help.