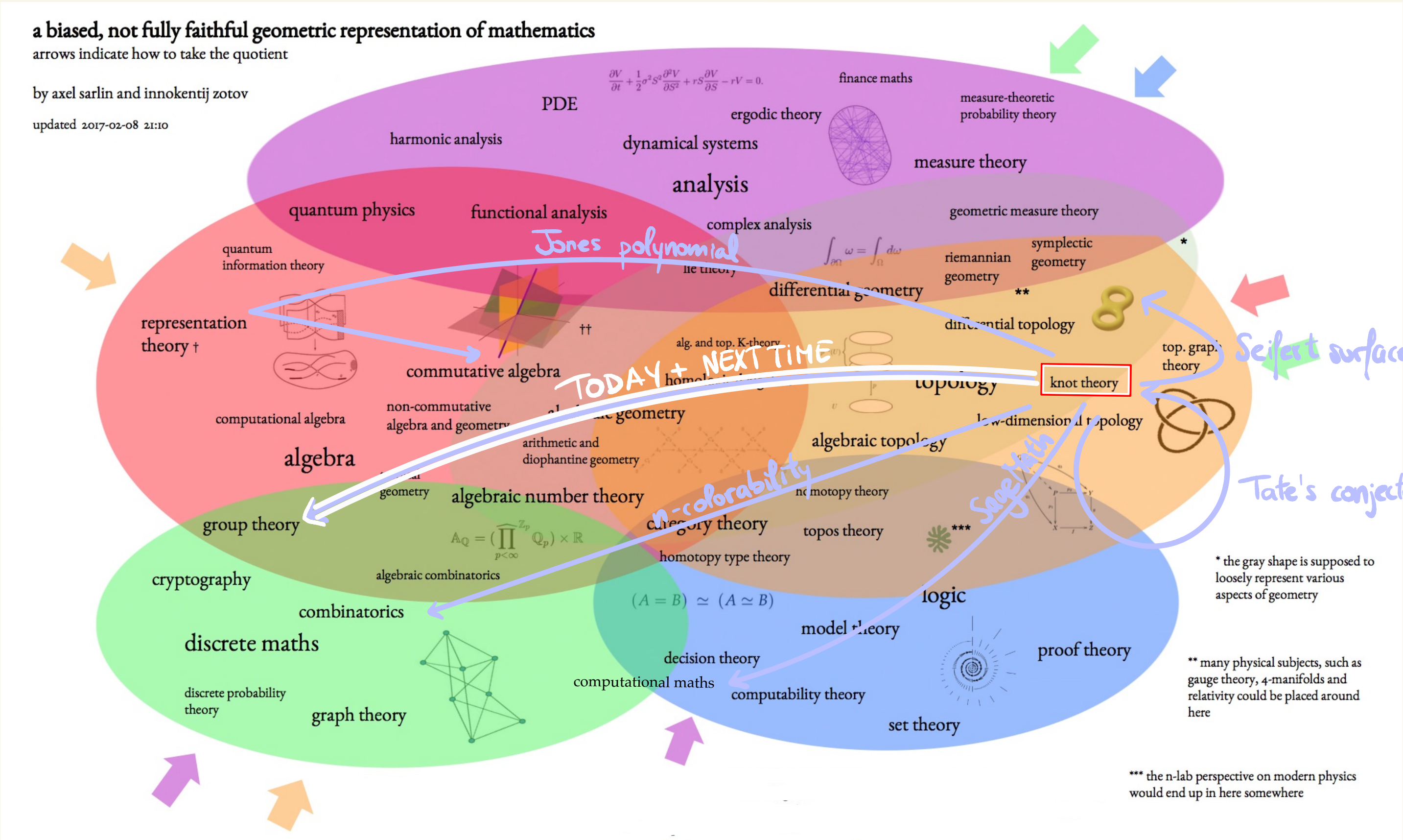
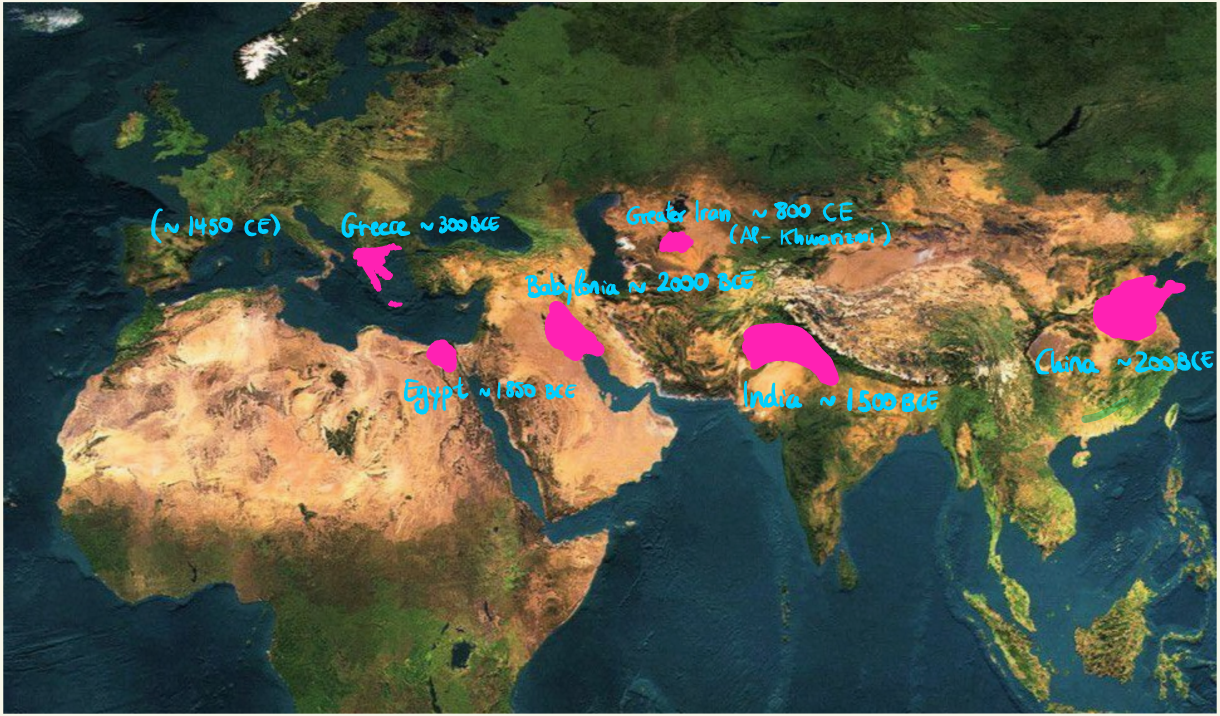
Reminder of knot theory so far:



11. A lightning introduction to group theory

Some history: $\quad ax^2+bx+c=0 \quad \rightsquigarrow \quad x=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$ "Modern notation"



Documented evidence of solutions to the quadratic equation, various degrees of abstraction.

$$ax^3 + bx^2 + cx + d = 0$$

Scipione del Ferro (1465 - 1526) : $x = \left\{ \begin{array}{l} x_0 \\ x_1 \\ x_2 \end{array} \right.$

$$x_k = -\frac{1}{3a}\left(b + \xi^k C + \frac{\Delta_0}{\Delta_1} \right)$$

where $C = \sqrt[3]{\dfrac{\Delta_1 + \sqrt{\Delta_1^2 - 4\Delta_0^3}}{2}}$

$$\Delta_0 = b^2 - 3ac$$

$$\Delta_1 = 2b^3 - 9abc + 27a^2 d$$

$$\xi = \frac{1 + \sqrt{-3}}{2}$$

... in words though.

$ax^4+bx^3+cx^2+dx+e=0$

Lodovico Ferrari (1522-1565)

Horrible but completely solved.

Summary of Ferrari's method [edit]

Given the quartic equation

$$Ax^4+Bx^3+Cx^2+Dx+E=0,$$

its solution can be found by means of the following calculations:

$$\alpha=-\frac{3B^2}{8A^2}+\frac{C}{A},$$

$$\beta=\frac{B^3}{8A^3}-\frac{BC}{2A^2}+\frac{D}{A},$$

$$\gamma=-\frac{3B^4}{256A^4}+\frac{CB^2}{16A^3}-\frac{BD}{4A^2}+\frac{E}{A}.$$

If $\beta=0$, then

$$x=-\frac{B}{4A}\pm_s\sqrt{\frac{-\alpha\pm_t\sqrt{\alpha^2-4\gamma}}{2}} \qquad (\text{for } \beta=0 \text{ only}).$$

Otherwise, continue with

$$P=-\frac{\alpha^2}{12}-\gamma,$$

$$Q=-\frac{\alpha^3}{108}+\frac{\alpha\gamma}{3}-\frac{\beta^2}{8},$$

$$R=-\frac{Q}{2}\pm\sqrt{\frac{Q^2}{4}+\frac{P^3}{27}},$$

(either sign of the square root will do)

$$U=\sqrt[3]{R},$$

(there are 3 complex roots, any one of them will do)

$$y=-\frac{5}{6}\alpha+\begin{cases}U=0 & \to -\sqrt[3]{Q}\\ U\neq 0, & \to U-\frac{P}{3U},\end{cases}$$

$$W=\sqrt{\alpha+2y}$$

$$x=-\frac{B}{4A}+\frac{\pm_s W\pm_t\sqrt{-\left(3\alpha+2y\pm_s\frac{2\beta}{W}\right)}}{2}.$$

The two $\pm_s$ must have the same sign, the $\pm_t$ is independent. To get all roots, compute x for $\pm_s,\pm_t$ = +,+ and for +,−; and for −,+ and for −,−. This formula handles repeated roots without problem.

Ferrari was the first to discover one of these labyrinthinesolutions[citation needed]. The equation which he solved was

$$x^4+6x^2-60x+36=0$$

which was already in depressed form. It has a pair of solutions which can be found with the set of formulas shown above.

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

300 years pass, many failed attempts (including Euler)

Niels Henrik Abel (1802 - 1829) : proof that there is no general formula in degree 5 (hence any degree)

tuberculosis

Still, some equations could be solved, but which ones?

Evariste Galois (1811 - 1832) : A complete answer to the question

(affair with friend's gf ⇝ duel, apparently)

- Worked for all degrees, all possible polynomials
- Elegant answer, deep study of symmetry
- Focuses on structure, rather than calculation. Marks the beginning of contemporary algebra

In particular, he jump-started the field of Group Theory

Group Theory basics

Definition: a set is a collection of objects, without repetitions.

Examples: $\{0, 1, 2\}$, $\{$ prime knots $\}$, $\{$ real numbers $\}$

finite   infinite   very infinite

The objects inside the sets are called elements, and whenever an element a belongs to a set A, we write $a \in A$.

Examples: $1 \in \{0, 1, 2, 3, \dots\}$

 $\notin$ $\{$ knots with genus 2 $\}$

Definition: a group is a set G together with an operation $*$ satisfying the following axioms:

- For all $x, y \in G$, $x * y \in G$. Closure
- For all $x, y, z \in G$
$$(x*y)*z = x*(y*z)$$
Associativity
- There exists an element $e \in G$, such that for all $x \in G$,
$$x*e = x \quad \text{and} \quad e*x = x$$
Identity element
- For all $x \in G$ there exists an element $y \in G$ such that
$$x*y = e \quad \text{and} \quad y*x = e$$
Inverse

We write it x^{-1}

Q?

This generalizes many notions you already know:

- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ with $* = +$

  Closure:

  Associativity:

  Unit element:

  Inverses:

- $\mathbb{R}_{>0} = \{$ positive real numbers $\}$ with $* = \cdot$

  Closure:

  Associativity:

  Unit element:

  Inverses:

Q?

- $\{ \text{True}, \text{False} \}$ with $* = \text{XOR}$

  Closure:

  Associativity:

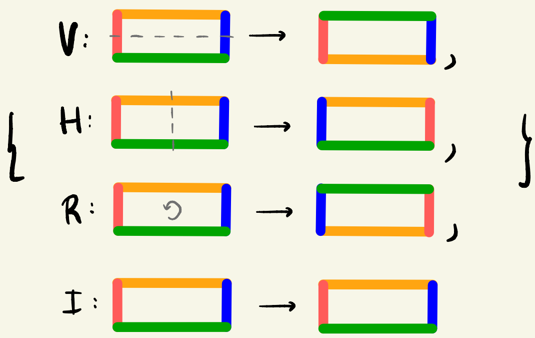
  Unit element:

  Inverses:

XOR	F	T
F	F	T
T	T	F

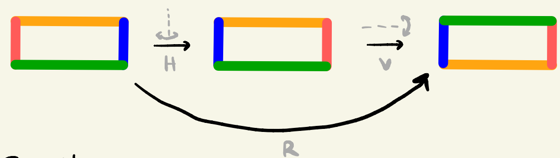
"Operation table"

- Symmetries of a rectangle:



, $* =$ composition of symmetries:

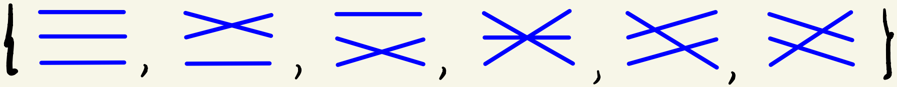
$V * H$:

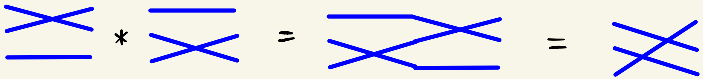


so $V * R = H$

Q?

- Symmetric group on 3 strands, $*$ = concatenation : "S_3"



Example : 

Closure: 6 possibilities, all drawn

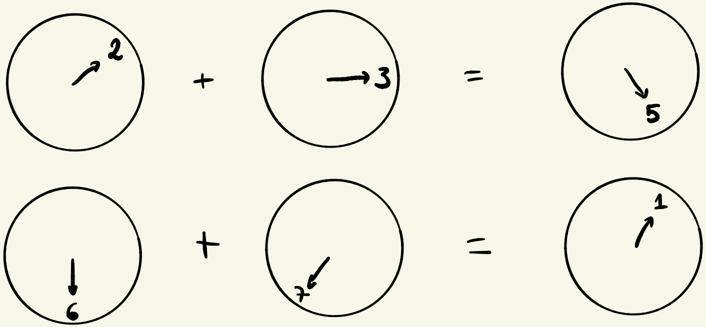
Associativity :

Unit element :

Inverses :

- Cyclic group with 12 elements: "C_{12}"

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, $\quad * = +$ (mod 12)



Closure:

Associativity:

Unit element:

Inverses:

Some nonexamples:

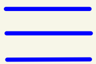
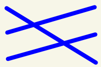
- $\mathbb{Z}$, $* = -$

  Closure:

  Associativity: Q

  Unit element:

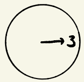
  Inverses:

- $\{$  ,  $\}$

  Q: what fails here?

Some notions for the exercises:

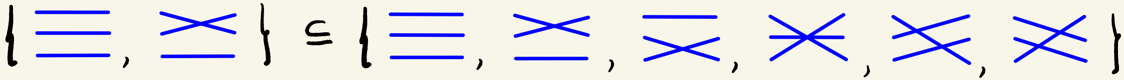
Definition: let g be an element of a group. The order of g, $\mathrm{ord}(g)$ is defined as the least power n such that $g^n = e$. If no such power exists we say $\mathrm{ord}(g) = \infty$.

Example: if $3 =$  in C_{12} then $\mathrm{ord}(3) = 4$

Definition: a subset A of a set B is another set whose elements are all contained in B. We write $A \subseteq B$.

Example: $\mathbb{R}_{>0} \subseteq \mathbb{R}$

Definition: a subgroup H of G is a subset $H \subseteq G$ with the same operation which is itself a group

Example: 

Q?

<u>Exercises</u>: investigate these examples, and more