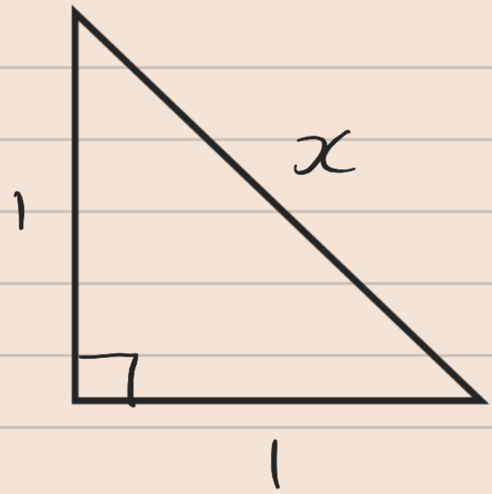
# Arithmetic, Geometry & Polynomials in the Variable q

Bailey Whitbread.

## PART I: Arithmetic




### ① An old problem:

Pythagoras' theorem.

$$x^2 = 2.$$

Let's give the equation a name.

$$A: \quad x^2 - 2 = 0$$

What are its solutions?

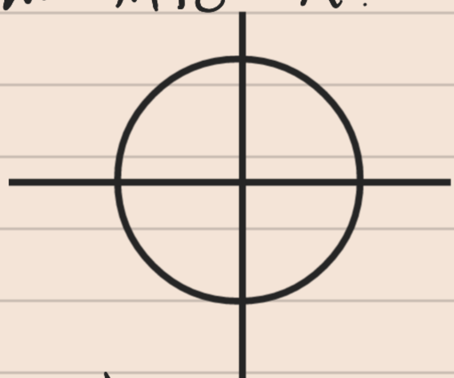
Some notation: $A(\text{Set}) := \{ \alpha \in \text{Set} \mid \alpha^2 - 2 = 0 \}$.

$\rightarrow A(\mathbb{Z}) = \emptyset$ $\qquad$ $\rightarrow A(\mathbb{R}) = \{\pm\sqrt{2}\}$.

$\rightarrow A(\mathbb{Q}) = \emptyset$ $\qquad$ $\rightarrow A(\mathbb{C}) = \{\pm\sqrt{2}\}$.

These sets are "shadows of A" in the sense that they yield insight into A.

### ② A geometric problem:



$$B: \quad x^2 + y^2 - 1 = 0$$

Again, $B(\text{Set}) := \{ (\alpha, \beta) \in \text{Set}^2 \mid \alpha^2 + \beta^2 - 1 = 0 \}$.

$\rightarrow B(\mathbb{Z}) = \{ (0, \pm 1), (\pm 1, 0) \}$.

$\rightarrow B(\mathbb{R}) = \{ (\cos\theta, \sin\theta) \mid \theta \in [0, 2\pi) \}$ manifold

$\rightarrow B(\mathbb{C}) = \{ (x, \pm\sqrt{1-x^2}) \mid x \in \mathbb{C} \}$ complex surface

$\rightarrow B(\mathbb{Q})$:

rational coords.

Every point arises from a Pythag triple. (up to sign).

Say $\alpha^2 + \beta^2 = \gamma^2$, $\alpha, \beta, \gamma \in \mathbb{Z}$

$$\rightsquigarrow \left(\frac{\alpha}{\gamma}\right)^2 + \left(\frac{\beta}{\gamma}\right)^2 = 1.$$

These are wildly different shadows with their own interesting geometry.

## 3 A familiar equation:

$C: \ ad - bc - 1 = 0$

$\rightarrow C(\mathbb{R}) = \{ (a,b,c,d) \in \mathbb{R}^4 \mid ad - bc - 1 = 0 \}$

$$\xleftrightarrow[\text{bij}]{} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \,\middle|\, \det = 1 \right\}$$

$\rightarrow C(\mathbb{R}) = SL_2(\mathbb{R})$, $C(\mathbb{C}) = SL_2(\mathbb{C})$.
$C(\mathbb{Q}) = SL_2(\mathbb{Q})$, $C(\mathbb{Z}) = SL_2(\mathbb{Z})$,

Shadows of $SL_2$

## (4) More matrix groups:

Recall $SO_2(\mathbb{R})$ equals

$$\left\{ X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \,\middle|\, XX^T = Id,\ \det X = 1 \right\}.$$

$$XX^T = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id$$

$$\rightsquigarrow SO_2 : \left\{ \begin{array}{l} a^2+b^2-1=0 \\ ac+bd=0 \\ c^2+d^2-1=0 \\ ad-bc-1=0 \end{array} \right\}.$$

All your favourite matrix groups are obtained as the solutions of polynomials.

$GL_n$, $SL_n$, $O_n$, $SU_n$, $Sp_{2n}$, $UT_n$, ...

(algebraic groups).

## Part II: Geometry

Fix a (Riemann surface) $\Sigma$ and an algebraic group $G$.

eg. $\Sigma =$ , $G = GL_n$.

# What can we do with this data?

① Solve Yang-Mills equations "for" $\Sigma_i$ & $G$.

A generalisation of Maxwell's equations.

This is $d_A^* F_A = 0$, a PDE.

Not for talk

- → $P$ = principle $G$-bundle over $\Sigma_i$.
- → $A$ = a connection on $P$.
- → $F_A$ = the curvature form on $A$.
- → $d_A^*$ = adjoint of $d_A$, the exterior covariant derivative.

② Solve Hitchin's self-duality equations "for" $\Sigma_i$ & $G$.

A dimension reduction of YM.

③ Prove the Geometric Langland's Conjecture "for" $\Sigma_i$ & $G$.

- → S-duality (of QF and/or string theories). eg. Montonen-Olive duality (generalises the electric-magnetic duality)
- → Number theoretic LLC related to Fermat's Last Theorem: $x^n + y^n = z^n$.

Not for talk

$$\left\{ \begin{matrix} G\text{-local sys} \\ \text{on } \Sigma_i \end{matrix} \right\} / \text{iso} \overset{\text{bij}}{\longleftrightarrow} \left\{ \begin{matrix} \text{Hecke eigensheaves} \\ \text{on } [G^\vee\text{-bundles of } \Sigma_i] \end{matrix} \right\}$$

④ Prove mirror symmetry "for" $\Sigma_1$ & $G$.

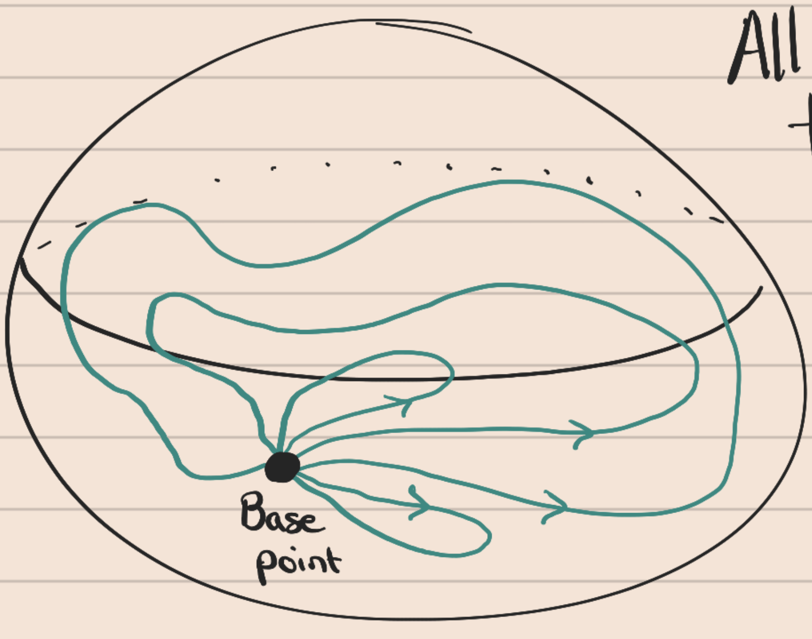
Symplectic geometry of a Calabi-Yau manifold $Y$ $\simeq$ Complex geometry of its mirror C-Y manifold $Y'$.

There is one object related to all of these problems, the 'representation space'

$$R := \mathrm{Hom}(\pi_1(\Sigma_1), G).$$

What is $\pi_1(\Sigma_1)$? A group describing the "essentially" different paths on $\Sigma_1$.

Ex 1 $\Sigma_1$ = Sphere.



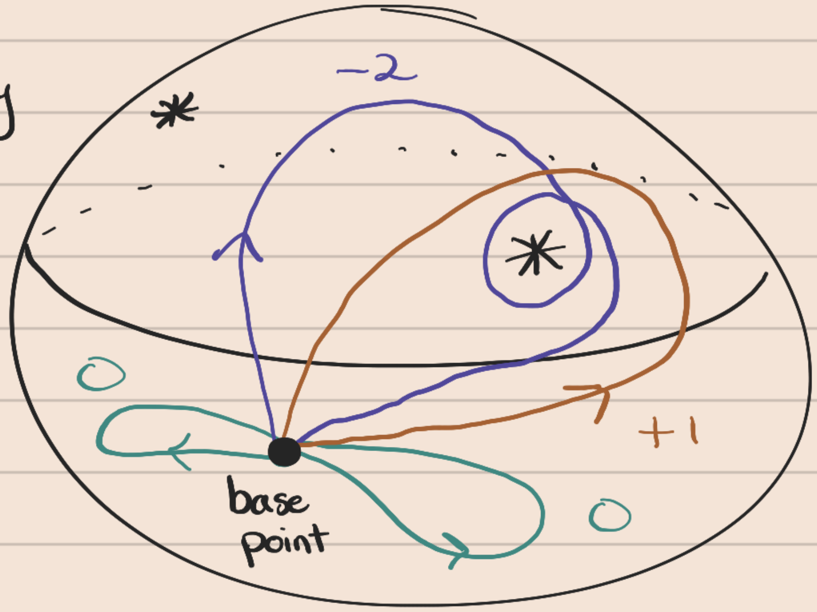

All essentially the same.

$\pi_1(\Sigma_1)$ = trivial gp

## Ex 2

$\Sigma_1' =$ Sphere minus two pts

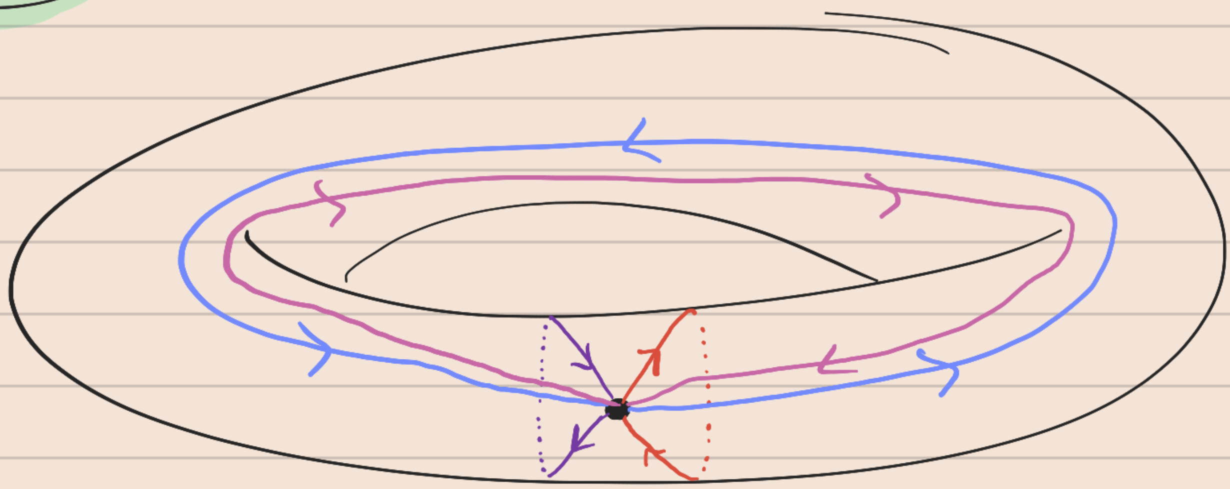
A loop is essentially determined by the # of loops & the direction around the puncture.




$\pi_1(\Sigma_1') \simeq (\mathbb{Z}, +)$.

## Ex 3

$\Sigma_1' =$ Torus



$\pi_1(\Sigma_1') \simeq \mathbb{Z} \times \mathbb{Z}$.

The groups $\pi_1(\Sigma_1')$ are all finitely generated.

eg. $\mathbb{Z} \times \mathbb{Z} = \langle a, b \mid ab = ba \rangle$.

$= \{1, a, a^2, \dots, b, b^2, \dots, ab, a^2b, ab^2, a^2b^2, \dots\}$

## What is $R$? $(\Sigma_1' = \text{Torus})$.

$$R = \mathrm{Hom}(\pi_1(\Sigma_1'), G)$$

$$\overset{\text{bij}}{\longleftrightarrow} \{ (X, Y) \in G^2 \mid XY = YX \} \subseteq G^2.$$

$$\rightsquigarrow R(\text{Set}) = \mathrm{Hom}\big(\pi_1(\Sigma_1'), G(\text{set})\big) \subseteq G(\text{Set})^2$$

**Eg.** Set $= \mathbb{C}$, $G = SL_2$.

$$R(\mathbb{C}) = \{ (A, B) \in SL_2(\mathbb{C})^2 \mid AB = BA \}.$$

Similarly, may look at $R(\mathbb{Q})$, $R(\mathbb{Z})$ etc.

If $\Sigma_1' =$ genus $g$ torus with $k$ punctures then $\pi_1(\Sigma_1')$ is fin. gen'd.

## Part III: Polynomials in the variable $q$

Reminder:

Understand $R := \mathrm{Hom}(\pi_1(\Sigma_1'), G)$ $\rightsquigarrow$ Understand YM, Hit. SDE, GLLC, Mir. Sym.

# How do we understand $R$?

We look at its shadows.

The Weil conjectures (proven) tell us there are some extremely important shadows:

$$R(\mathbb{F}_q),$$

$\mathbb{F}_q :=$ the finite field of size $q = p^k$.

(Thm: A finite field of size $n$ exists iff $n$ is a prime power. Moreover, exactly one such field exists (up to isomorphism.))

$\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_8, \mathbb{F}_9, \mathbb{F}_{11}, \ldots$

$\mathbb{F}_p$ is just $\mathbb{Z}_p$

$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. (modular arithmetic)

In $\mathbb{F}_q$, we have $+, -, \times, \div$ ie. arithmetic.

eg. $\mathbb{Z}_3 = \mathbb{F}_3 = \{0, 1, 2\}$. $2 + 1 = 0$

$2 \times 2 = 1$. etc.

The Weil conjectures tell us to understand the numbers

$$|R(\mathbb{F}_q)| =: f(q).$$

<u>Theorem:</u> [Katz] If $f$ is a polynomial in the variable $q$, then this polynomial encodes cohomological information about $R(\mathbb{C})$.

<u>In particular,</u>

- dim $R(\mathbb{C})$ = degree of $f$.
- Euler characteristic of $R(\mathbb{C})$ = $f(1)$.
- # of connected components of $R(\mathbb{C})$ = leading coeff of $f$.

This works for many varieties, not just $R$.

eg. projective space.

$$\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$$

$$|\mathbb{P}^n(\mathbb{F}_q)| = |\mathbb{A}^n(\mathbb{F}_q)| + |\mathbb{A}^{n-1}(\mathbb{F}_q)| + \dots + |\mathbb{A}^1(\mathbb{F}_q)| + |\mathbb{A}^0(\mathbb{F}_q)|$$

$$= q^n + q^{n-1} + \dots + q + 1. = f(q).$$

- $\dim \mathbb{P}(\mathbb{C}) = n$
- Euler char of $\mathbb{P}(\mathbb{C})$ $= 1 + \dots + 1 = n+1.$
- # of conn comp $= 1$ (ie. $\mathbb{P}^n$ is conn.).

Returning to $R = \mathrm{Hom}(\pi_1(\Sigma_1^1), SL_2)$:

$$|R(\mathbb{F}_q)| = \left|\left\{(A,B) \in SL_2(\mathbb{F}_q)^2 \,\middle|\, AB = BA\right\}\right|$$

Frob. Massform.

$$= |SL_2(\mathbb{F}_q)| \times \#\text{ of irred. reps of } SL_2(\mathbb{F}_q).$$

If $\Sigma_1 =$ genus $g$ torus then,

$$|R(\mathbb{F}_q)| = \frac{1}{|SL_2(\mathbb{F}_q)|} \sum_{\substack{\chi \text{ irrep} \\ \text{of } SL_2(\mathbb{F}_q)}} \left(\frac{|SL_2(\mathbb{F}_q)|}{\dim \chi}\right)^{2g-2}.$$

Frob. mass form.

true for $G = GL_n, PGL_n, SO_n, Sp_{2n}, \dots$