

Scratchwork: Torus Orbits

A common step in contemporary number theory literature is to re-define the problem as a group theory problem... Especially using “torus orbits”.

Linear algebra works over any field, K . So we just say “let K be a field...” and if we have a single plane $\mathbb{R}^m \subseteq \mathbb{R}^n$ we know more-or-less they all behave the same. In fact, rational planes $\mathbb{Q}^m \subseteq \mathbb{Q}^n$ are not all identical.

$$X(\mathbb{Q}) = \{x^2 + y^2 = 1\} \subseteq \mathbb{Q}^2$$

This is a \mathbb{Q} -torus. Are there any rational points on this circle? I can name $(0, \pm 1)$ and $(\pm 1, 0)$. Here are two more:

$$\left(\frac{3}{5}, \frac{4}{5}\right), \left(\frac{5}{13}, \frac{12}{13}\right) \in X(\mathbb{Q})$$

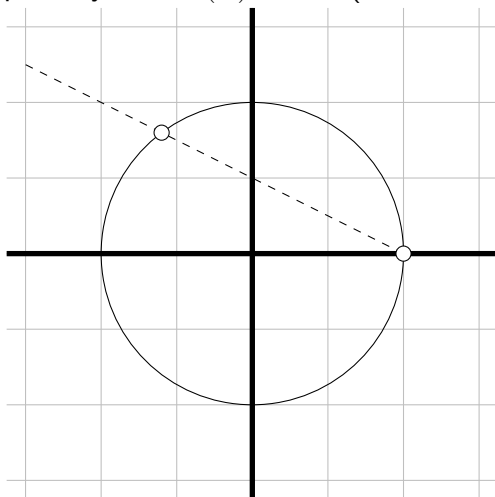
Since the circle was defined using algebra, we can say it is a **variety**. In fact, $X(\mathbb{Q})$ forms a group:

$$\left(\frac{3}{5} + i\frac{4}{5}\right)^2 = \left(\frac{3^2 - 4^2}{25}\right) + 2 \times \left(\frac{3 \times 4}{25}\right)i = -\frac{7}{25} + i\frac{24}{25}$$

Or we could use 2×2 matrices. There's a way find a 2×2 matrix solution to $x^2 + 1 = 0$. E.g. $(x, y) \mapsto (-y, x)$.

$$\begin{bmatrix} \frac{3}{5} & -\frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{bmatrix}^2 = \begin{bmatrix} \frac{7}{25} & -\frac{24}{25} \\ \frac{24}{25} & \frac{7}{25} \end{bmatrix}$$

This tells us the Pythagorean triples form a *multiplicative group*, but also we are looking for a \mathbb{Q} -action, and possibly an $\mathrm{SL}_2(\mathbb{Z})$ action (I read it's actually a $\Gamma(2)$ action.)



Notice we've used a tiny bit of degree theory $[\text{circle}] \cdot [\text{line}] = 2$. This **is** an instance of cohomology¹ and we don't bother giving it a fancy name. This is called **stereographic projection**, I think?

$$\begin{aligned} |(1, 0) + (t, mt)|^2 &= (t+1)^2 + mt^2 = 1 \\ t &= (1, 0), \left(\frac{1-m^2}{m^2+1}, -\frac{2m}{m^2+1}\right) \end{aligned}$$

¹intersection theory

with $m = \frac{a}{b} \in \mathbb{Q}$. These become $[a^2 - b^2 : 2ab : a^2 + b^2]$ over \mathbb{Z} as a proportion. Multiplying by the slope $m \mapsto qx$ could lead to a reasonable group action of \mathbb{Q}^\times on \mathbb{Q} .

Ex Show no such \mathbb{Q}^\times action exists on $\mathrm{SO}_2(x^2 + y^2, \mathbb{Q})$.

In fact, showing that *no* isomorphism (or group) action exists might be quite hard. Now I just want to soak in that SO_2 for various quadratic forms are now quite different. This is how we can talk about **rational quadratic forms**.

$$\begin{aligned}\mathrm{SO}_2(x^2 + y^2, \mathbb{Q}) &\not\simeq \mathrm{SO}_2(x^2 + 2y^2, \mathbb{Q}) \not\simeq \mathrm{SO}_2(x^2 - 2y^2, \mathbb{Q}) \\ \mathrm{SO}_2(x^2 + y^2, \mathbb{R}) &\simeq \mathrm{SO}_2(x^2 + 2y^2, \mathbb{R}) \not\simeq \mathrm{SO}_2(x^2 - 2y^2, \mathbb{R})\end{aligned}$$

since we do have $\sqrt{2} \in \mathbb{R}$, but not $\sqrt{-2} \in \mathbb{R}$. So letting the quadratic form $q \in M_{2 \times 2}(\mathbb{Q})$ vary we can obtain lots of different infinite abelian groups, roughly the size of \mathbb{Q}^\times . These are called \mathbb{Q} -tori and if there was such an isomorphism – the matrices could be diagonalized over \mathbb{Q} – then these would be called **split torus**.

Here is another torus built to the same variety $X = \{x^2 + y^2 - 1 = 0\}$ a circle. Let's consider $X(\mathbb{Q}(\sqrt{2}))$. The points on the circle living in the field $\mathbb{Q}[x]/(x^2 - 2)$. Since $\sqrt{2} \notin \mathbb{Q}$ this is a slightly bigger field and we have “more” points. Nonetheless

$$\overline{\mathbb{Q}} = \overline{\mathbb{Q}(\sqrt{2})} = \mathbb{R} \rightarrow X(\mathbb{Q}) \subseteq X(\mathbb{Q}(\sqrt{2})) \subseteq X(\mathbb{R}) \rightarrow \overline{X(\mathbb{Q})} = \overline{X(\mathbb{Q}(\sqrt{2}))} = X(\mathbb{R})$$

What allows us to make that conclusion so easily? The closure operation $\overline{(\cdot)}$ comes from **topology** – basically a way of deciding which sets of points are “close” or “nearby” or “related” or “approximate”.

$$\begin{aligned}(a_1 + a_2\sqrt{2})^2 + (b_1 + b_2\sqrt{2})^2 &= (c_1 + c_2\sqrt{2})^2 \\ (a_1^2 + 2a_2^2) + (b_1^2 + 2b_2^2) &= (c_1^2 + 2c_2^2) \\ a_1a_2 + b_1b_2 &= c_1c_2\end{aligned}$$

And usually there's some trick that I'm overlooking. Hopefully we can find a reading of these equations from within Euclidean Geometry, where this equation originated.

Ex Let's try solving $x^2 + y^2 + z^2 = n$ as a torus orbit of some kind. This exercise is worked out in a handful of places.² I'm going to ask for the automorphic representation π of $\mathrm{SL}_2(\mathbb{A})$ for a spherical harmonic $\phi \in L^2(\mathrm{SO}_3)$.

How do theta-functions occur as automorphic representations? This is possibly called the “Weil representation” or the “Metaplectic” representation.³ I'll concede that Waldspurger formula has been known since 1980, but his derivation takes about 30 or 40 pages and he never “evaluates” the thing. It's on me, to define this term **evaluate**.

Conversely, since equidistribution statements (i.e. uniform distribution of points on S^2) is so hard, we can find statements about the uniform distribution and say that our solutions $X(\mathbb{Z}, n)$ are “close to” being examples of inputs. There could be a whole theory of not-quite-uniform points on the 2-sphere

Paul Nelson works through this in 2016, and it looks like Waldspurger's computations – and *he* says these calculations are new. So change is pretty slow.

²My standard for well-known is that everybody knows it. There are only 20000 practicing mathematicians in the US, maybe a tenth of those are number theorists. So...

³However, when talking to professors (or reading their work) there's a steep cliff separating the people who know the Automorphic Forms jargon and the people who do not. And even another cliff between factions of professions (e.g. Automorphic Forms and Number Theory). This is a social network analysis (SNA) phenomenon...

Ex Find a sequence of rational numbers $x_n \in \mathbb{Q}$ converging to $\sqrt{2} \in \mathbb{R}$ and $\sqrt{-1} \in \mathbb{Q}_5$.

$$\left| \left(\frac{p}{q} \right)^2 - 2 \right|_{\mathbb{R}} < \epsilon_1 \text{ and } \left| \left(\frac{p}{q} \right)^2 + 1 \right|_5 < \epsilon_2$$

Let's make sure the second one exists. $2^2 + 1 = 5 \in 5\mathbb{Z}$ and $3^2 + 1 = 2 \times 5 \in 5\mathbb{Z}$. This tell us there should be two numbers $x_{\pm} = \sqrt{-1} \in \mathbb{Q}_5$ by Hensel's Lemma (basically Taylor formula).

$$\text{diag} : \frac{p}{q} \in \mathbb{Q} \rightarrow \left(\frac{p}{q}, \frac{p}{q} \right) \in \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{R} \times \mathbb{Q}_5$$

I don't have a great notation for it. $\overline{\text{diag}(\mathbb{Q} \times \mathbb{Q})} = \mathbb{R} \times \mathbb{Q}_5$. The algebra is telling us by attempting to *define* the word "diagonal" or the density of \mathbb{Q} in such a big space as $\mathbb{R} \times \mathbb{Q}_5$ we've missed something even bigger.

Ex Let's try to quantify how dense the rational points are on the circle? Let's find a $k \in \mathbb{Z}$ such that:

$$\min_{(p,q) \in \mathbb{Z}} \left| \left(\frac{1}{\sqrt{2}} - \frac{p}{q} \right)^2 + \left(\frac{1}{\sqrt{2}} - \frac{p}{q} \right)^2 \right| \asymp q^k$$

Just a thought.

References

- [1] David Witte Morris **Introduction to Arithmetic Groups** arXiv:math/0106063
- [2] John Voight **Quaternion Algebras** (v.0.9.13) <https://math.dartmouth.edu/~jvoight/quat.html>
- [3] Jean-Loupe Waldspurger **Sur les Valeurs de Certaines Fonctions L Automorphes en leur Centre de Symétrie** Compositio Mathematica 54.2 (1985): 173-242. <<http://eudml.org/doc/89702>>.
- [4] Paul D Nelson **The spectral decomposition of $|\theta|^2$** arXiv:1601.02529