Points and conics

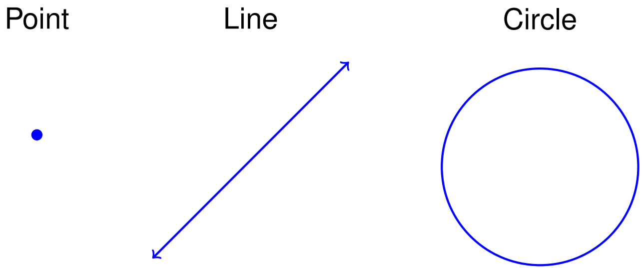
Asher Auel

Department of Mathematics
Yale University

University of Connecticut
Math Club
March 12th, 2014

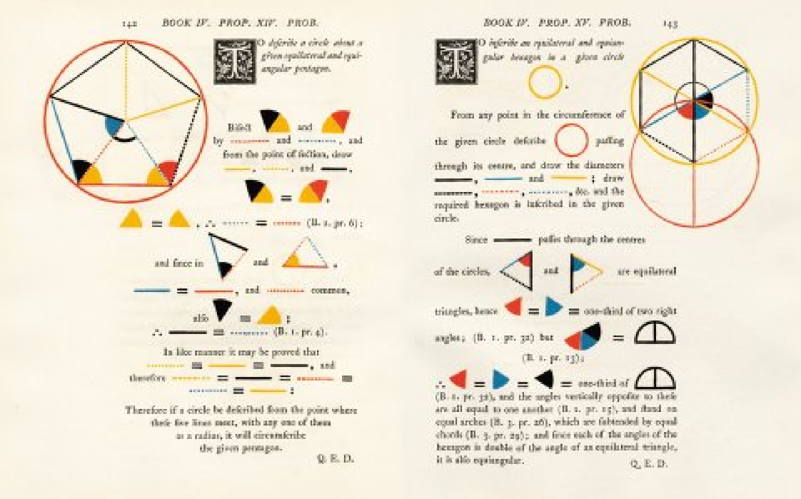
Plane Geometry

Euclid, -300



Plane Geometry

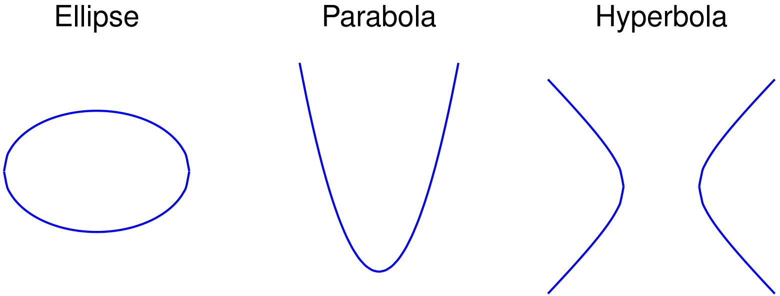
Euclid, -300



Oliver Byrne “The Elements of Euclid” 1847

Conic sections

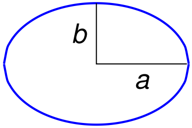
Apollonius, -200



Conic sections

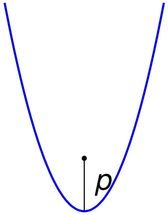
Apollonius, -200

Ellipse



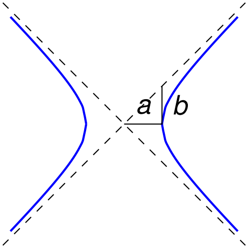
$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

Parabola



$$y = \frac{x^2}{4p}$$

Hyperbola



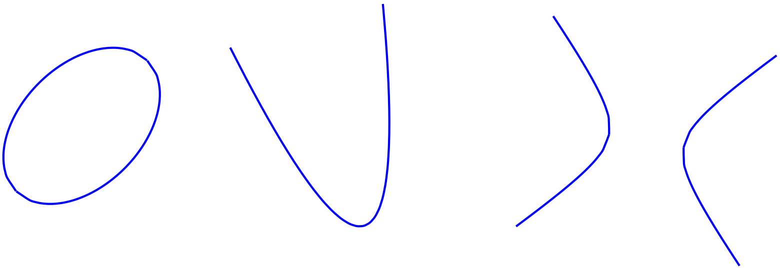
$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

Canonical forms

Conic sections

Apollonius, -200

Ellipse Parabola Hyperbola

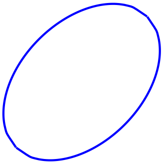


$$A\,x^2 + B\,xy + C\,y^2 + D\,x + E\,y + F = 0$$

Conic sections

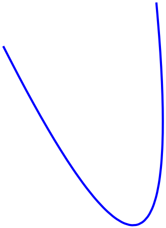
Apollonius, -200

Ellipse



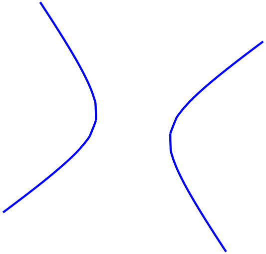
$B^2 - 4AC < 0$

Parabola



$B^2 - 4AC = 0$

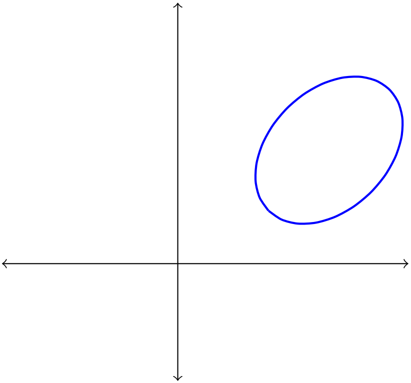
Hyperbola



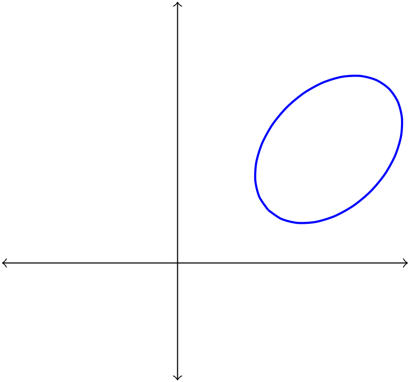
$B^2 - 4AC > 0$

$$A\,x^2 + B\,xy + C\,y^2 + D\,x + E\,y + F = 0$$

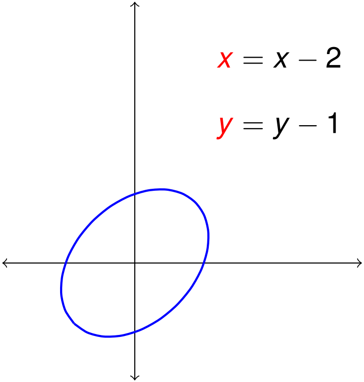
$$4x^2 - 2xy + 4y^2 - 14x - 4y + 15 = 0$$



$$4x^2 - 2xy + 4y^2 - 14x - 4y + 15 = 0$$



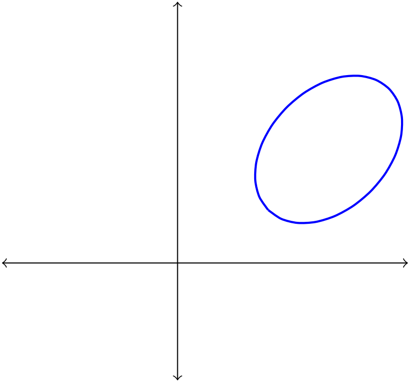
$$4x^2 - 2xy + 4y^2 = 1$$



$$x = x - 2$$

$$y = y - 1$$

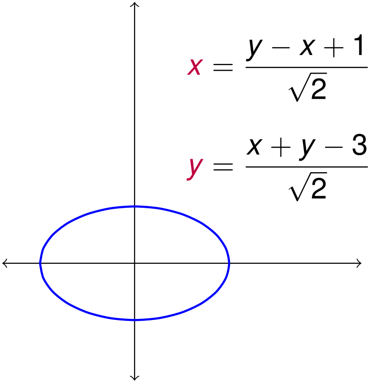
$$4x^2 - 2xy + 4y^2 - 14x - 4y + 15 = 0$$



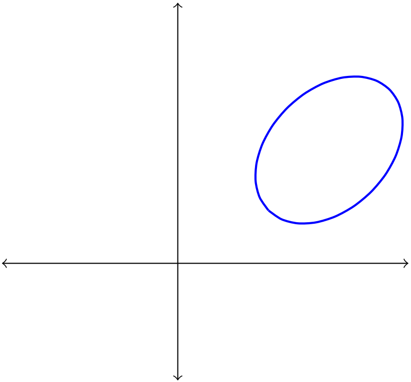
$$3x^2 + 5y^2 = 1$$

$$x = \frac{y - x + 1}{\sqrt{2}}$$

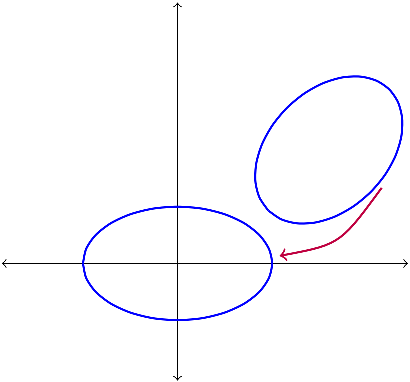
$$y = \frac{x + y - 3}{\sqrt{2}}$$



$$4x^2 - 2xy + 4y^2 - 14x - 4y + 15 = 0$$



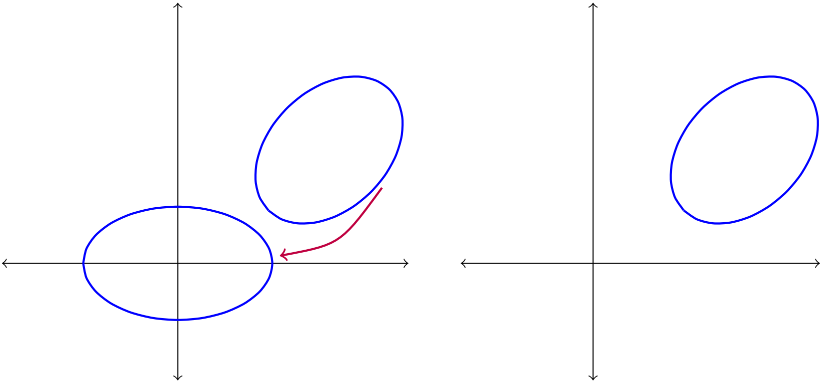
$$4x^2 - 2xy + 4y^2 - 14x - 4y + 15 = 0$$



$$3x^2 + 5y^2 = 1$$

euclidean
transformation

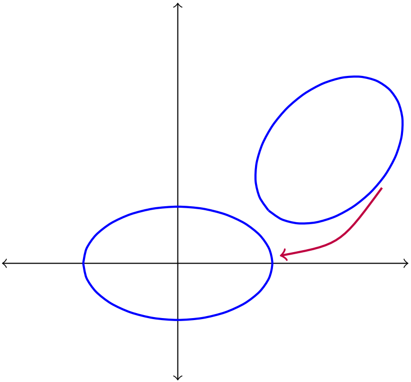
$$4x^2 - 2xy + 4y^2 - 14x - 4y + 15 = 0$$

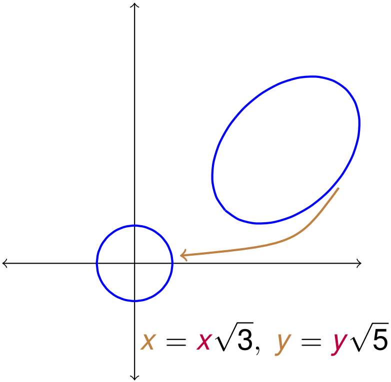


$$3x^2 + 5y^2 = 1$$

euclidean
transformation

$$4x^2 - 2xy + 4y^2 - 14x - 4y + 15 = 0$$





$$3x^2 + 5y^2 = 1$$

$$x^2 + y^2 = 1$$

euclidean transformation

general affine transformation

General Affine Equivalence

$$q(x, y) = A\,x^2 + B\,xy + C\,y^2 + D\,x + E\,y + F$$
$$q'(x, y) = A'\,x^2 + B'\,xy + C'\,y^2 + D'\,x + E'\,y + F'$$

General Affine Equivalence

$$q(x,y) = A\,x^2 + B\,xy + C\,y^2 + D\,x + E\,y + F$$
$$q'(x,y) = A'\,x^2 + B'\,xy + C'\,y^2 + D'\,x + E'\,y + F'$$

$$q(x,y) \approx q'(x,y)$$

$$\Longleftrightarrow$$

$$q(x,y) = c \cdot q'(sx + ty + w, ux + vy + w')$$

General Affine Equivalence

$$q(x,y) = A\,x^2 + B\,xy + C\,y^2 + D\,x + E\,y + F$$
$$q'(x,y) = A'\,x^2 + B'\,xy + C'\,y^2 + D'\,x + E'\,y + F'$$

$$q(x,y) \approx q'(x,y)$$

$$\Longleftrightarrow$$

$$\begin{aligned} q(x,y) &= c \cdot q'(sx + ty + w, ux + vy + w') \\ &= c \cdot q'\left(\begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} w \\ w' \end{pmatrix} \right) \end{aligned}$$

General Affine Equivalence

$$q(x,y) = A\,x^2 + B\,xy + C\,y^2 + D\,x + E\,y + F$$
$$q'(x,y) = A'\,x^2 + B'\,xy + C'\,y^2 + D'\,x + E'\,y + F'$$

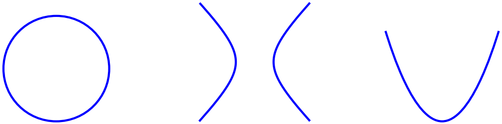
$$q(x,y) \approx q'(x,y)$$

$$\Longleftrightarrow$$

$$\begin{aligned} q(x,y) &= c \cdot q'(sx + ty + w, ux + vy + w') \\ &= c \cdot q'\left(\begin{pmatrix} s & t \\ u & v \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} w \\ w' \end{pmatrix}\right) \end{aligned}$$

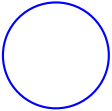
Example: $4x^2 - 2xy + 4y^2 - 14x - 4y + 15 \;\approx\; x^2 + y^2 - 1$

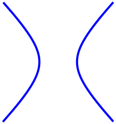
General Affine Classification

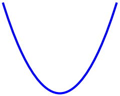


$x^2 + y^2 = 1$ $\qquad$ $x^2 - y^2 = 1$ $\qquad$ $y = x^2$

General Affine Classification





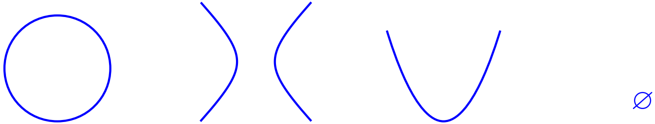


$\varnothing$

$x^2 + y^2 = 1$ $x^2 - y^2 = 1$ $y = x^2$ $x^2 + y^2 = -1$

General Affine Classification

smooth/singular

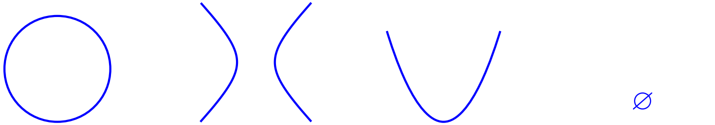


$x^2 + y^2 = 1$ $\quad$ $x^2 - y^2 = 1$ $\quad$ $y = x^2$ $\quad$ $x^2 + y^2 = -1$

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

General Affine Classification

smooth/singular

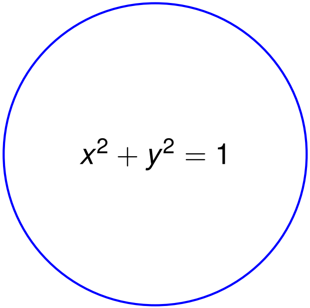


$x^2 + y^2 = 1$ $\quad$ $x^2 - y^2 = 1$ $\quad$ $y = x^2$ $\quad$ $x^2 + y^2 = -1$

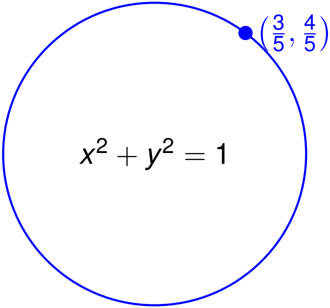
$x^2 + y^2 = 0$ $\quad$ $x^2 - y^2 = 0$ $\quad$ $y^2 = 0$ $\quad$ $y^2 = 1$

We'll focus on smooth conics.

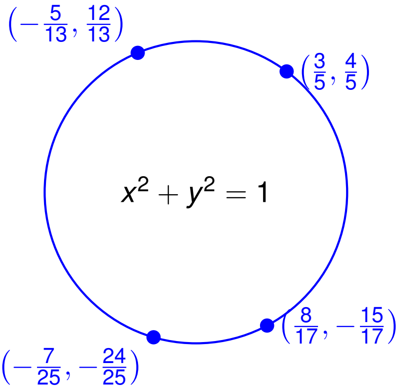
Rational Points



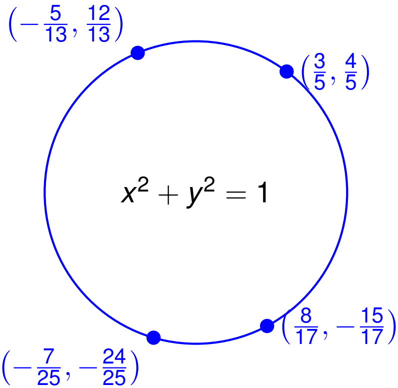
Rational Points



Rational Points



Rational Points



Rational point $\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$ $\iff$ Pythagorean triple $3^2 + 4^2 = 5^2$

General Affine Equivalence over $\mathbb{Q}$

$\mathbb{Q} = \left\{ \frac{a}{b} \ : \ a, b \text{ integers}, \ b \neq 0 \right\}$ set of rational numbers

$$q(x, y) \approx_{\mathbb{Q}} q'(x, y)$$

$$\Longleftrightarrow$$

$$\begin{aligned} q(x, y) &= c \cdot q'(sx + ty + w, ux + vy + w') \\ &= c \cdot q' \left(\begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} w \\ w' \end{pmatrix} \right) \end{aligned}$$

Where we only allow:

$$c \neq 0 \in \mathbb{Q}, \qquad \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Q}), \qquad \begin{pmatrix} w \\ w' \end{pmatrix} \in \mathbb{Q}^2$$

General Affine Equivalence over $\mathbb{Q}$

$\mathbb{Q} = \left\{ \frac{a}{b} \;:\; a, b \text{ integers}, \; b \neq 0 \right\}$ set of rational numbers

$$q(x, y) \approx_{\mathbb{Q}} q'(x, y)$$

$$\Longleftrightarrow$$

$$\begin{aligned} q(x, y) &= c \cdot q'(sx + ty + w, ux + vy + w') \\ &= c \cdot q'\left(\begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} w \\ w' \end{pmatrix} \right) \end{aligned}$$

Where we only allow:

$$c \neq 0 \in \mathbb{Q}, \qquad \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Q}), \qquad \begin{pmatrix} w \\ w' \end{pmatrix} \in \mathbb{Q}^2$$

Main point: General affine equivalence over $\mathbb{Q}$ gives a bijection on the sets of rational points.

Example. $4x^2 - 2xy + 4y^2 - 14x - 4y + 15 \ \overset{?}{\approx}_{\mathbb{Q}} \ x^2 + y^2 - 1$

Example. $4x^2 - 2xy + 4y^2 - 14x - 4y + 15 \overset{?}{\approx}_{\mathbb{Q}} x^2 + y^2 - 1$

$$4x^2 - 2xy + 4y^2 - 14x - 4y + 15 \approx_{\mathbb{Q}} 4x^2 - 2xy + 4y^2 - 1$$

Remember $x = x - 2, \quad y = y - 1$

Example. $4x^2 - 2xy + 4y^2 - 14x - 4y + 15 \overset{?}{\approx}_{\mathbb{Q}} x^2 + y^2 - 1$

$$\begin{aligned} 4x^2 - 2xy + 4y^2 - 14x - 4y + 15 &\approx_{\mathbb{Q}} 4x^2 - 2xy + 4y^2 - 1 \\ &\approx_{\mathbb{Q}} 6x^2 + 10y^2 - 1 \end{aligned}$$

$$x = \frac{1}{2}(y - x + 1), \quad y = \frac{1}{2}(x + y - 3)$$

Example. $4x^2 - 2xy + 4y^2 - 14x - 4y + 15 \overset{?}{\approx}_{\mathbb{Q}} x^2 + y^2 - 1$

$$\begin{aligned} 4x^2 - 2xy + 4y^2 - 14x - 4y + 15 &\approx_{\mathbb{Q}} 4x^2 - 2xy + 4y^2 - 1 \\ &\approx_{\mathbb{Q}} 6x^2 + 10y^2 - 1 \end{aligned}$$

$q(x, y) = A\,x^2 + B\,xy + C\,y^2 + D\,x + E\,y + F$

Discriminant $\Delta(q) = B^2 - 4AC$

Lemma. $q(x, y) \approx_{\mathbb{Q}} q'(x, y) \implies \Delta(q) = d^2 \Delta(q')$ for $d \in \mathbb{Q}$.

Example. $4x^2 - 2xy + 4y^2 - 14x - 4y + 15 \overset{?}{\approx}_{\mathbb{Q}} x^2 + y^2 - 1$

$$\begin{aligned} 4x^2 - 2xy + 4y^2 - 14x - 4y + 15 &\approx_{\mathbb{Q}} 4x^2 - 2xy + 4y^2 - 1 \\ &\approx_{\mathbb{Q}} 6x^2 + 10y^2 - 1 \end{aligned}$$

$q(x, y) = A\,x^2 + B\,xy + C\,y^2 + D\,x + E\,y + F$

Discriminant $\Delta(q) = B^2 - 4AC$

Lemma. $q(x, y) \approx_{\mathbb{Q}} q'(x, y) \implies \Delta(q) = d^2\Delta(q')$ for $d \in \mathbb{Q}$.

Corollary. $4x^2 - 2xy + 4y^2 - 14x - 4y + 15 \not\approx_{\mathbb{Q}} x^2 + y^2 - 1$

compare $\Delta \quad -60 \neq -4d^2$

$\sqrt{15}$ irrational

Example. $x^2 + y^2 + 1 \not\approx_{\mathbb{Q}} x^2 + y^2 - 1$ yet both have $\Delta = 4$.

$x^2 + y^2 = -1$ has no rational solutions
$x^2 + y^2 = 1$ has many rational solutions

Example. $x^2 + y^2 + 1 \not\approx_{\mathbb{Q}} x^2 + y^2 - 1$ yet both have $\Delta = 4$.

$x^2 + y^2 = -1$ has no rational solutions
$x^2 + y^2 = 1$ has many rational solutions

Conclusion. The discriminant Δ does not necessarily distinguish between general affine equivalence classes over $\mathbb{Q}$.

Diagonalization

Theorem. Every smooth conic over $\mathbb{Q}$ is equivalent to:

$$y = x^2 \qquad \text{or} \qquad a\,x^2 + b\,y^2 = 1, \quad \text{for some } a, b \in \mathbb{Q}$$

Diagonalization

Theorem. Every smooth conic over $\mathbb{Q}$ is equivalent to:

$$y = x^2 \qquad \text{or} \qquad a\,x^2 + b\,y^2 = 1, \quad \text{for some } a, b \in \mathbb{Q}$$

Proof. Case $\Delta \neq 0$ (not a parabola).

$$q(x,y) = A\,x^2 + B\,xy + C\,y^2 + D\,x + E\,y + F$$

Can always clear away the linear terms with a translation by solutions to the system of linear equations:

$$\frac{\partial}{\partial x} q(x,y) = \frac{\partial}{\partial y} q(x,y) = 0 \;\Leftrightarrow\; \begin{cases} 2Ax + By &= -D \\ Bx + 2Cy &= -E \end{cases}$$

$$\begin{aligned} q(x,y) &\approx_{\mathbb{Q}} A\,x^2 + B\,xy + C\,y^2 + F' \\ &= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + F \\ &\approx_{\mathbb{Q}} \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} s & t \\ u & v \end{pmatrix}^{\mathrm{t}} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + F \end{aligned}$$

Diagonalization

Theorem. Every smooth conic over $\mathbb{Q}$ is equivalent to:

$$y = x^2 \qquad \text{or} \qquad a\,x^2 + b\,y^2 = 1, \quad \text{for some } a, b \in \mathbb{Q}$$

Proof.

$$q(x,y) \approx_{\mathbb{Q}} \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} s & t \\ u & v \end{pmatrix}^{\mathrm{t}} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + F$$

A “diagonalization” problem. Over $\mathbb{R}$, this can be done by the spectral theorem in linear algebra “every real symmetric matrix can be diagonalized by an orthogonal matrix” (remember Q is orthogonal if $Q^{\mathrm{t}} = Q^{-1}$). Over $\mathbb{Q}$ this is the higher theory of “completing the square.”

Clifford–Hasse–Witt symbol

Theorem. Every smooth conic over $\mathbb{Q}$ is equivalent to:

$$y = x^2 \qquad \text{or} \qquad a\,x^2 + b\,y^2 = 1, \quad \text{for some } a, b \in \mathbb{Q} \setminus \{0\}$$

Clifford–Hasse–Witt symbol

Theorem. Every smooth conic over $\mathbb{Q}$ is equivalent to:

$$y = x^2 \qquad \text{or} \qquad a\,x^2 + b\,y^2 = 1, \quad \text{for some } a, b \in \mathbb{Q} \smallsetminus \{0\}$$

Clifford–Hasse–Witt symbol

$$q(x,y) \approx_{\mathbb{Q}} ax^2 + by^2 - 1 \quad \mapsto \quad [a, b]$$
$$q(x,y) \approx_{\mathbb{Q}} y - x^2 \quad \mapsto \quad [1, -1]$$

(*A priori* depends on the choice of diagonalization.)

Clifford–Hasse–Witt symbol

Theorem. Every smooth conic over $\mathbb{Q}$ is equivalent to:

$$y = x^2 \qquad \text{or} \qquad a\,x^2 + b\,y^2 = 1, \quad \text{for some } a, b \in \mathbb{Q} \setminus \{0\}$$

Clifford–Hasse–Witt symbol

$$\begin{aligned} q(x,y) \approx_{\mathbb{Q}} ax^2 + by^2 - 1 \quad &\mapsto \quad [a,b] \\ q(x,y) \approx_{\mathbb{Q}} y - x^2 \quad &\mapsto \quad [1,-1] \end{aligned}$$

Properties:

- $[a,b] \approx_{\mathbb{Q}} [b,a]$ $\qquad (x,y) \mapsto (y,x)$
- $[a,b] \approx_{\mathbb{Q}} [a,b\,c^2]$ $\qquad (x,y) \mapsto (x,cy)$
- $[a,-a] \approx_{\mathbb{Q}} [1,-1]$ $\qquad \binom{x}{y} \mapsto \frac{1}{4}\begin{pmatrix} a+1 & a-1 \\ a-1 & a+1 \end{pmatrix}\binom{x}{y}$
- $[a,1-a] \approx_{\mathbb{Q}} [1,-1]$ $\qquad$ more tricky

Manipulating symbols

Properties:

- $[a, b] \approx_{\mathbb{Q}} [b, a]$
- $[a, b] \approx_{\mathbb{Q}} [a, b\,c^2]$
- $[a, -a] \approx_{\mathbb{Q}} [1, -1]$
- $[a, 1 - a] \approx_{\mathbb{Q}} [1, -1]$

Manipulating symbols

Properties:

- $[a, b] \approx_{\mathbb{Q}} [b, a]$
- $[a, b] \approx_{\mathbb{Q}} [a, b\,c^2]$
- $[a, -a] \approx_{\mathbb{Q}} [1, -1]$
- $[a, 1 - a] \approx_{\mathbb{Q}} [1, -1]$
- $[a, u^2 - av^2] \approx_{\mathbb{Q}} [1, -1]$ for any $u, v \in \mathbb{Q}$ with $u^2 - av^2 \neq 0$

Manipulating symbols

Properties:

- $[a, b] \approx_{\mathbb{Q}} [b, a]$
- $[a, b] \approx_{\mathbb{Q}} [a, b\,c^2]$
- $[a, -a] \approx_{\mathbb{Q}} [1, -1]$
- $[a, 1-a] \approx_{\mathbb{Q}} [1, -1]$
- $[a, u^2 - av^2] \approx_{\mathbb{Q}} [1, -1]$ for any $u, v \in \mathbb{Q}$ with $u^2 - av^2 \neq 0$

$$S(\mathbb{Q}) = \{[a, b]\ :\ a, b \in \mathbb{Q} \setminus \{0\}\}/ \approx_{\mathbb{Q}} \text{ properties}$$

Manipulating symbols

Properties:

- $[a, b] \approx_{\mathbb{Q}} [b, a]$
- $[a, b] \approx_{\mathbb{Q}} [a, b\,c^2]$
- $[a, -a] \approx_{\mathbb{Q}} [1, -1]$
- $[a, 1-a] \approx_{\mathbb{Q}} [1, -1]$
- $[a, u^2 - av^2] \approx_{\mathbb{Q}} [1, -1]$ for any $u, v \in \mathbb{Q}$ with $u^2 - av^2 \neq 0$

$$S(\mathbb{Q}) = \{[a, b] \,:\, a, b \in \mathbb{Q} \smallsetminus \{0\}\} / \approx_{\mathbb{Q}} \text{ properties}$$

Example. For any $a \in \mathbb{Q} \smallsetminus \{0\}$ we have

$$[1, a] \approx_{\mathbb{Q}} [a, 1] \approx_{\mathbb{Q}} [a, 1^2 - a\,0^2] \approx_{\mathbb{Q}} [1, -1]$$

in $S(\mathbb{Q})$. The class of $[1, -1]$ is called the trivial symbol.

Manipulating symbols

Properties:

- $[a, b] \approx_{\mathbb{Q}} [b, a]$
- $[a, b] \approx_{\mathbb{Q}} [a, b\,c^2]$
- $[a, -a] \approx_{\mathbb{Q}} [1, -1]$
- $[a, 1-a] \approx_{\mathbb{Q}} [1, -1]$
- $[a, u^2 - av^2] \approx_{\mathbb{Q}} [1, -1]$ for any $u, v \in \mathbb{Q}$ with $u^2 - av^2 \neq 0$

$$S(\mathbb{Q}) = \{[a, b] \,:\, a, b \in \mathbb{Q} \setminus \{0\}\}/ \approx_{\mathbb{Q}} \text{ properties}$$

Lemma. The Clifford–Hasse–Witt symbol of $q(x, y)$, taken in $S(\mathbb{Q})$, doesn't depend on the general affine equivalence class.

$$\{\text{conics}\}/ \approx_{\mathbb{Q}} \;\longrightarrow\; S(\mathbb{Q})$$

Hasse–Minkowski Theorem

$c, c' \in \mathbb{Q}$ are in the same square class if $c = d^2 c'$ for $d \in \mathbb{Q}$

$\Delta(\mathbb{Q})$ set of rational square classes (including 0)

$S(\mathbb{Q})$ set of symbols up to manipulations by properties

Hasse–Minkowski Theorem

$c, c' \in \mathbb{Q}$ are in the same square class if $c = d^2 c'$ for $d \in \mathbb{Q}$

$\Delta(\mathbb{Q})$ set of rational square classes (including 0)

$S(\mathbb{Q})$ set of symbols up to manipulations by properties

Theorem (Hasse–Minkowski). A conic over $\mathbb{Q}$ is uniquely determined, up to general affine equivalence, by its discriminant in $\Delta(\mathbb{Q})$ and its Clifford–Hasse–Witt symbol in $S(\mathbb{Q})$.

Hasse–Minkowski Theorem

$c, c' \in \mathbb{Q}$ are in the same square class if $c = d^2 c'$ for $d \in \mathbb{Q}$

$\Delta(\mathbb{Q})$ set of rational square classes (including 0)

$S(\mathbb{Q})$ set of symbols up to manipulations by properties

Theorem (Hasse–Minkowski). A conic over $\mathbb{Q}$ is uniquely determined, up to general affine equivalence, by its discriminant in $\Delta(\mathbb{Q})$ and its Clifford–Hasse–Witt symbol in $S(\mathbb{Q})$.

Recall. The trivial symbol is the class of $[1, -1]$ in $S(\mathbb{Q})$.

Theorem. A conic over $\mathbb{Q}$ has a rational point if and only if its Clifford–Hasse–Witt symbol is trivial in $S(\mathbb{Q})$.

Recall. The trivial symbol is the class of $[1, -1]$ in $S(\mathbb{Q})$.

Theorem. A conic over $\mathbb{Q}$ has a rational point if and only if its Clifford–Hasse–Witt symbol is trivial in $S(\mathbb{Q})$.

Recall. The trivial symbol is the class of $[1, -1]$ in $S(\mathbb{Q})$.

Theorem. A conic over $\mathbb{Q}$ has a rational point if and only if its Clifford–Hasse–Witt symbol is trivial in $S(\mathbb{Q})$.

Example. Does

$$q(x, y) = 4x^2 - 2xy + 4y^2 - 14x - 4y + 15 = 0$$

have a rational point?
To use the theorem, we already calculated

$$q(x, y) \quad \approx_{\mathbb{Q}} \quad 6x^2 + 10y^2 - 1 \quad \mapsto \quad [6, 10]$$

Note that $10 = 4^2 - 6 \cdot 1^2$, so $[6, 10] = [1, -1]$ is trivial in $S(\mathbb{Q})$.
So $q(x, y) = 0$ has a rational point?

Recall. The trivial symbol is the class of $[1, -1]$ in $S(\mathbb{Q})$.

Theorem. A conic over $\mathbb{Q}$ has a rational point if and only if its Clifford–Hasse–Witt symbol is trivial in $S(\mathbb{Q})$.

Example. Does

$$q(x, y) = 4x^2 - 2xy + 4y^2 - 14x - 4y + 15 = 0$$

have a rational point?
To use the theorem, we already calculated

$$q(x, y) \quad \approx_{\mathbb{Q}} \quad 6x^2 + 10y^2 - 1 \quad \mapsto \quad [6, 10]$$

Note that $10 = 4^2 - 6 \cdot 1^2$, so $[6, 10] = [1, -1]$ is trivial in $S(\mathbb{Q})$.
So $q(x, y) = 0$ has a rational point?

$$6\left(\frac{1}{4}\right)^2 + 10\left(\frac{1}{4}\right)^2 = 1$$

$$4 \cdot 2^2 - 2 \cdot 2 \cdot \frac{3}{2} + 4\left(\frac{3}{2}\right)^2 - 14 \cdot 2 - 4\frac{3}{2} + 15 = 0$$

Legendre's Theorem

$ax^2 + by^2 = 1$ has a solution in rationals $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$

$$\iff$$

$aX^2 + bY^2 = Z^2$ has a solution in integers X, Y, Z

Legendre's Theorem

$ax^2 + by^2 = 1$ has a solution in rationals $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$

$$\iff$$

$aX^2 + bY^2 = Z^2$ has a solution in integers X, Y, Z

Theorem (Legendre's Theorem). Let a and b be positive squarefree integers. Then

$$aX^2 + bY^2 = Z^2$$

has a nontrivial solution if and only if a is a square modulo b and b is a square modulo a and $-\frac{ab}{d^2}$ is a square modulo d (here $d = \gcd(a, b)$).

Quaternions

Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication

$$i^2 = j^2 = k^2 = ijk = -1$$

& cut it on a stone of this bridge.

Quaternions

Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication

$$i^2 = j^2 = k^2 = ijk = -1$$

& cut it on a stone of this bridge.

$$\mathbb{R} \quad \rightsquigarrow \quad \mathbb{C} = \mathbb{R} + i\,\mathbb{R}$$

Quaternions

Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication

$$i^2 = j^2 = k^2 = ijk = -1$$

& cut it on a stone of this bridge.

$$\mathbb{R} \quad \rightsquigarrow \quad \mathbb{C} = \mathbb{R} + i\,\mathbb{R} \quad \rightsquigarrow \quad \mathbb{H} = \mathbb{R} + i\,\mathbb{R} + j\,\mathbb{R} + k\,\mathbb{R}$$

Quaternions

Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication

$$i^2 = j^2 = k^2 = ijk = -1$$

& cut it on a stone of this bridge.

$$\mathbb{R} \quad \rightsquigarrow \quad \mathbb{C} = \mathbb{R} + i\,\mathbb{R} \quad \rightsquigarrow \quad \mathbb{H} = \mathbb{R} + i\,\mathbb{R} + j\,\mathbb{R} + k\,\mathbb{R}$$

not ordered

Quaternions

Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication

$$i^2 = j^2 = k^2 = ijk = -1$$

& cut it on a stone of this bridge.

$\mathbb{R}$ $\rightsquigarrow$ $\mathbb{C} = \mathbb{R} + i\,\mathbb{R}$ $\rightsquigarrow$ $\mathbb{H} = \mathbb{R} + i\,\mathbb{R} + j\,\mathbb{R} + k\,\mathbb{R}$

not ordered — not commutative

Quaternions

Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication

$$i^2 = j^2 = k^2 = ijk = -1$$

& cut it on a stone of this bridge.

$$\mathbb{R} \quad \rightsquigarrow \quad \mathbb{C} = \mathbb{R} + i\,\mathbb{R} \quad \rightsquigarrow \quad \mathbb{H} = \mathbb{R} + i\,\mathbb{R} + j\,\mathbb{R} + k\,\mathbb{R}$$

not ordered — not commutative

$$ij = k, \quad jk = i, \quad ki = j, \quad ij = -ji, \quad ik = -ki, \quad jk = -kj$$

Skew-fields

Skew-field: $\mathbb{F}$ set with operations $+$ and $\cdot$ satisfying:

- Associativity: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  $x + (y + z) = (x + y) + z$
- Distributivity: $x \cdot (y + z) = x \cdot y + x \cdot z$
- Identity: $0 + x = x = x + 0$
  $1 \cdot x = x = x \cdot 1$
- Inverses: $\exists -x, \quad x + (-x) = (-x) + x = 0$
  $x \neq 0 \quad \Rightarrow \quad \exists\, x^{-1}, \quad x \cdot x^{-1} = x^{-1} \cdot x = 1$
- Commutativity: $x + y = y + x$

Skew-fields

Skew-field: $\mathbb{F}$ set with operations $+$ and $\cdot$ satisfying:

- Associativity: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  $x + (y + z) = (x + y) + z$
- Distributivity: $x \cdot (y + z) = x \cdot y + x \cdot z$
- Identity: $0 + x = x = x + 0$
  $1 \cdot x = x = x \cdot 1$
- Inverses: $\exists -x, \quad x + (-x) = (-x) + x = 0$
  $x \neq 0 \quad \Rightarrow \quad \exists\, x^{-1}, \quad x \cdot x^{-1} = x^{-1} \cdot x = 1$
- Commutativity: $x + y = y + x$
  $x \cdot y \neq y \cdot x$

Inverting Quaternions

$$(1 + i + j)\left(\frac{1}{3} - \frac{1}{3}i - \frac{1}{3}j\right) = \frac{1}{3} + \frac{1}{3} + \frac{1}{3} + 0 = 1$$

Inverting Quaternions

$$(1 + i + j)\left(\frac{1}{3} - \frac{1}{3}i - \frac{1}{3}j\right) = \frac{1}{3} + \frac{1}{3} + \frac{1}{3} + 0 = 1$$

$$(1 + i + 2j)\left(\frac{1}{6} - \frac{1}{6}i - \frac{1}{3}j\right) = \frac{1}{6} + \frac{1}{6} + \frac{2}{3} + 0 = 1$$

Inverting Quaternions

$$(1 + i + j)\left(\frac{1}{3} - \frac{1}{3}i - \frac{1}{3}j\right) = \frac{1}{3} + \frac{1}{3} + \frac{1}{3} + 0 = 1$$

$$(1 + i + 2j)\left(\frac{1}{6} - \frac{1}{6}i - \frac{1}{3}j\right) = \frac{1}{6} + \frac{1}{6} + \frac{2}{3} + 0 = 1$$

Quaternion conjugation:

$$(x + yi + zj + wk)(x - yi - zj - wk) = x^2 + y^2 + z^2 + w^2$$

Inverting Quaternions

$$(1+i+j)\left(\frac{1}{3}-\frac{1}{3}i-\frac{1}{3}j\right)=\frac{1}{3}+\frac{1}{3}+\frac{1}{3}+0=1$$

$$(1+i+2j)\left(\frac{1}{6}-\frac{1}{6}i-\frac{1}{3}j\right)=\frac{1}{6}+\frac{1}{6}+\frac{2}{3}+0=1$$

Quaternion conjugation:

$$(x+yi+zj+wk)(x-yi-zj-wk)=x^2+y^2+z^2+w^2$$

$$\boxed{(x+yi+zj+wk)^{-1}=\frac{x-yi-zj-wk}{x^2+y^2+z^2+w^2}}$$

$$x^2+y^2+z^2+w^2=0 \quad \Leftrightarrow \quad x=y=z=w=0$$

Applications

Euclidean 3-space

Quantum Mechanics

Applications

Euclidean 3-space Imaginary quaternions

$$\mathbb{R}^3 \hookrightarrow \mathbb{H}$$

$$\vec{v} = (v_1, v_2, v_3) \mapsto v = v_1\, i + v_2\, j + v_3\, k$$

Quantum Mechanics

Applications

Euclidean 3-space Imaginary quaternions

$$\mathbb{R}^3 \hookrightarrow \mathbb{H}$$

$$\vec{v} = (v_1, v_2, v_3) \mapsto v = v_1\, i + v_2\, j + v_3\, k$$

$$v\, w = -\vec{v} \cdot \vec{w} + \vec{v} \times \vec{w}$$

Quantum Mechanics

Applications

Euclidean 3-space Imaginary quaternions

$$\mathbb{R}^3 \hookrightarrow \mathbb{H}$$

$$\vec{v} = (v_1, v_2, v_3) \mapsto v = v_1\, i + v_2\, j + v_3\, k$$

$$v\, w = -\vec{v} \cdot \vec{w} + \vec{v} \times \vec{w}$$

Quantum Mechanics Pauli matrices for fermionic spin (1920s):

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Applications

Euclidean 3-space Imaginary quaternions

$$\mathbb{R}^3 \hookrightarrow \mathbb{H}$$

$$\vec{v} = (v_1, v_2, v_3) \mapsto v = v_1\, i + v_2\, j + v_3\, k$$

$$v\, w = -\vec{v} \cdot \vec{w} + \vec{v} \times \vec{w}$$

Quantum Mechanics Pauli matrices for fermionic spin (1920s):

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$i \leftrightarrow \sigma_1\sigma_2, \quad j \leftrightarrow \sigma_3\sigma_1, \quad k \leftrightarrow \sigma_2\sigma_3$$

$$S^3 = \{q \in \mathbb{H} \ : \ q\,\overline{q} = 1\} \to \mathbf{SO}(3)$$

$$q \mapsto v \mapsto q\, v\, q^{-1}$$

Quaternions over $\mathbb{Q}$

Theorem (Frobenius 1877): $\mathbb{F}$ a (skew-)field, $\mathbb{R} \subset \mathbb{F}$ center, then $\mathbb{F}$ is either $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

Quaternions over $\mathbb{Q}$

Theorem (Frobenius 1877): $\mathbb{F}$ a (skew-)field, $\mathbb{R} \subset \mathbb{F}$ center, then $\mathbb{F}$ is either $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

Lots of different quaternion algebras over $\mathbb{Q}$.

Quaternions over $\mathbb{Q}$

Theorem (Frobenius 1877): $\mathbb{F}$ a (skew-)field, $\mathbb{R} \subset \mathbb{F}$ center, then $\mathbb{F}$ is either $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

Lots of different quaternion algebras over $\mathbb{Q}$.

$$\mathbb{H}_{\mathbb{Q}} = \{x + yi + zj + wk \in \mathbb{H} \ : \ x, y, z, w \in \mathbb{Q}\}$$

$$\mathbb{H}_{2,3} = \left\{ x+yi+zj+wk \ : \ \begin{array}{l} x, y, z, w \in \mathbb{Q} \\ i^2 = 2, j^2 = 3, k^2 = -6, ij = k, \ldots \end{array} \right\}$$

Quaternions over $\mathbb{Q}$

Theorem (Frobenius 1877): $\mathbb{F}$ a (skew-)field, $\mathbb{R} \subset \mathbb{F}$ center, then $\mathbb{F}$ is either $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

Lots of different quaternion algebras over $\mathbb{Q}$.

$$\mathbb{H}_{\mathbb{Q}} = \{x + yi + zj + wk \in \mathbb{H} \ : \ x, y, z, w \in \mathbb{Q}\}$$

$$\mathbb{H}_{2,3} = \left\{ x+yi+zj+wk \ : \ \begin{array}{l} x, y, z, w \in \mathbb{Q} \\ i^2 = 2, j^2 = 3, k^2 = -6, ij = k, \ldots \end{array} \right\}$$

Check invertibility:

$$(x + yi + zj + wk)(x - yi - zj - wk) = x^2 - 2y^2 - 3z^2 + 6w^2$$

$$x^2 - 2y^2 - 3z^2 + 6w^2 \stackrel{?}{=} 0$$

Quaternions over $\mathbb{Q}$

Theorem (Frobenius 1877): $\mathbb{F}$ a (skew-)field, $\mathbb{R} \subset \mathbb{F}$ center, then $\mathbb{F}$ is either $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

Lots of different quaternion algebras over $\mathbb{Q}$.

$$\mathbb{H}_{\mathbb{Q}} = \{x + yi + zj + wk \in \mathbb{H} \ : \ x, y, z, w \in \mathbb{Q}\}$$

$$\mathbb{H}_{2,3} = \left\{ x + yi + zj + wk \ : \ \begin{array}{l} x, y, z, w \in \mathbb{Q} \\ i^2 = 2, j^2 = 3, k^2 = -6, ij = k, \ldots \end{array} \right\}$$

Check invertibility:

$$(x + yi + zj + wk)(x - yi - zj - wk) = x^2 - 2y^2 - 3z^2 + 6w^2$$

$$x^2 - 2y^2 - 3z^2 + 6w^2 = 0 \Leftrightarrow \ x = y = z = w = 0$$

Exercise!

Quaternions over $\mathbb{Q}$

Theorem (Frobenius 1877): $\mathbb{F}$ a (skew-)field, $\mathbb{R} \subset \mathbb{F}$ center, then $\mathbb{F}$ is either $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

Lots of different quaternion algebras over $\mathbb{Q}$.

$$\mathbb{H}_{\mathbb{Q}} = \{x + yi + zj + wk \in \mathbb{H} \ : \ x, y, z, w \in \mathbb{Q}\}$$

$$\mathbb{H}_{2,3} = \left\{ x + yi + zj + wk \ : \ \begin{array}{l} x, y, z, w \in \mathbb{Q} \\ i^2 = 2, j^2 = 3, k^2 = -6, ij = k, \ldots \end{array} \right\}$$

Check invertibility:

$$(x + yi + zj + wk)(x - yi - zj - wk) = x^2 - 2y^2 - 3z^2 + 6w^2$$

$$x^2 - 2y^2 - 3z^2 + 6w^2 = 0 \Leftrightarrow \ x = y = z = w = 0$$

Exercise! Hint $(x^2 - 2y^2) - 3(z^2 - 2w^2)$

Hilbert symbol: $\mathbb{H}_{a,b}$ 4-dimensional algebra over $\mathbb{Q}$:

$$i^2 = a, \quad j^2 = b, \quad k^2 = -ab, \quad ij = k, \quad ij = -ji, \ldots$$

Hilbert symbol: $\mathbb{H}_{a,b}$ 4-dimensional algebra over $\mathbb{Q}$:

$$i^2 = a, \quad j^2 = b, \quad k^2 = -ab, \quad ij = k, \quad ij = -ji, \ldots$$

Is $\mathbb{H}_{a,b}$ a skew-field?

Hilbert symbol: $\mathbb{H}_{a,b}$ 4-dimensional algebra over $\mathbb{Q}$:

$$i^2 = a, \quad j^2 = b, \quad k^2 = -ab, \quad ij = k, \quad ij = -ji, \ldots$$

Is $\mathbb{H}_{a,b}$ a skew-field?

Check invertibility:

$$(x + yi + zj + wk)(x - yi - zj - wk) = x^2 - ay^2 - bz^2 + abw^2$$

Hilbert symbol: $\mathbb{H}_{a,b}$ 4-dimensional algebra over $\mathbb{Q}$:

$$i^2 = a, \quad j^2 = b, \quad k^2 = -ab, \quad ij = k, \quad ij = -ji, \ldots$$

Is $\mathbb{H}_{a,b}$ a skew-field?

Check invertibility:

$$(x + yi + zj + wk)(x - yi - zj - wk) = x^2 - ay^2 - bz^2 + abw^2$$

$\mathbb{H}_{1,1}$

Hilbert symbol: $\mathbb{H}_{a,b}$ 4-dimensional algebra over $\mathbb{Q}$:

$$i^2 = a, \quad j^2 = b, \quad k^2 = -ab, \quad ij = k, \quad ij = -ji, \ldots$$

Is $\mathbb{H}_{a,b}$ a skew-field?

Check invertibility:

$$(x + yi + zj + wk)(x - yi - zj - wk) = x^2 - ay^2 - bz^2 + abw^2$$

$\mathbb{H}_{1,1}$ $\quad x^2 - y^2 - z^2 + w^2 = 0$ often

Hilbert symbol: $\mathbb{H}_{a,b}$ 4-dimensional algebra over $\mathbb{Q}$:

$$i^2 = a, \quad j^2 = b, \quad k^2 = -ab, \quad ij = k, \quad ij = -ji, \ldots$$

Is $\mathbb{H}_{a,b}$ a skew-field?

Check invertibility:

$$(x + yi + zj + wk)(x - yi - zj - wk) = x^2 - ay^2 - bz^2 + abw^2$$

$\mathbb{H}_{1,1}$ $\quad x^2 - y^2 - z^2 + w^2 = 0$ often

$\mathbb{H}_{2,-1}$

Hilbert symbol: $\mathbb{H}_{a,b}$ 4-dimensional algebra over $\mathbb{Q}$:

$$i^2 = a, \quad j^2 = b, \quad k^2 = -ab, \quad ij = k, \quad ij = -ji, \ldots$$

Is $\mathbb{H}_{a,b}$ a skew-field?

Check invertibility:

$$(x + yi + zj + wk)(x - yi - zj - wk) = x^2 - ay^2 - bz^2 + abw^2$$

$\mathbb{H}_{1,1}$ $\quad x^2 - y^2 - z^2 + w^2 = 0$ often

$\mathbb{H}_{2,-1}$ $\quad x^2 - 2y^2 + z^2 - 2w^2 = 0$ often

Can $\mathbb{H}_{a,b} = \mathbb{H}_{c,d}$?

Can $\mathbb{H}_{a,b} = \mathbb{H}_{c,d}$?

Properties:

- $\mathbb{H}_{a,b} = \mathbb{H}_{b,a}$
- $\mathbb{H}_{a,b} = \mathbb{H}_{a,bc^2}$
- $\mathbb{H}_{a,-a} = \mathbb{H}_{1,-1}$

Can $\mathbb{H}_{a,b} = \mathbb{H}_{c,d}$?

Properties:

- $\mathbb{H}_{a,b} = \mathbb{H}_{b,a}$
- $\mathbb{H}_{a,b} = \mathbb{H}_{a,bc^2}$
- $\mathbb{H}_{a,-a} = \mathbb{H}_{1,-1}$

Theorem (Minkowski 1896, Merkurjev 1982): Every skew-field over $\mathbb{Q}$ is a Hilbert symbol $\mathbb{H}_{a,b}$.

Conics and Quaternions

Clifford–Hasse–Witt symbol $[a, b]$ and Hilbert symbol $\mathbb{H}_{a,b}$.

$$q(x, y) \approx ax^2 + by^2 = 1 \mapsto [a, b]$$

Conics and Quaternions

Clifford–Hasse–Witt symbol $[a, b]$ and Hilbert symbol $\mathbb{H}_{a,b}$.

$$q(x, y) \approx ax^2 + by^2 = 1 \mapsto [a, b]$$

Theorem: Conic sections and quaternion algebras over $\mathbb{Q}$ determine each other:

$$[a, b] \approx [c, d] \qquad \Leftrightarrow \qquad \mathbb{H}_{a,b} = \mathbb{H}_{c,d} \quad \text{and} \quad ab = cd \cdot e^2$$

Conics and Quaternions

Clifford–Hasse–Witt symbol $[a, b]$ and Hilbert symbol $\mathbb{H}_{a,b}$.

$$q(x, y) \approx ax^2 + by^2 = 1 \mapsto [a, b]$$

Theorem: Conic sections and quaternion algebras over $\mathbb{Q}$ determine each other:

$$[a, b] \approx [c, d] \qquad \Leftrightarrow \qquad \mathbb{H}_{a,b} = \mathbb{H}_{c,d} \quad \text{and} \quad ab = cd \cdot e^2$$

Idea: Connection between 2-dimensional conic section

$$ax^2 + by^2 = 1$$

and 4-dimensional "quaternion invertibility" conic section

$$x^2 - ay^2 - bz^2 + abw^2 = 0$$