Let $\mathbb{K}$ be a field.

A polynomial in 2 variables over $\mathbb{K}$, is expressed as

$$\boxed{f(x,y) = \sum_{\substack{0 \le i \le n \\ 0 \le j \le k}} a_{ij}\, x^i y^j}$$

where $a_{n,k} \neq 0$ and $a_{ij} \in \mathbb{K}$. The collection of all such polynomials is denoted $\mathbb{K}[x,y]$.

$\mathbb{K}[x,y]$ is also called a polynomial ring.

$$\Rightarrow \boxed{\mathbb{K}[x,y] = \mathbb{K}[x][y]}$$

We cannot have long division for multivariate polynomial rings.

~~Proof~~ $\forall f, g \in \mathbb{K}[x,y]$ $\exists$ $q, r \in \mathbb{K}[x,y]$ such that $f = gq + r$ where $\deg(r) < \deg(g)$.

When $f(x,y) = y$ and $g(x,y) = x$

$\exists\, q, r$ such that $y = xq + r$.

Since $deg(r) < deg(g) = 1$

$\Rightarrow deg(r) = 0$

$\Rightarrow r \in \mathbb{K}$.

Substituting $y = x = 0$, $r = 0$.

So $y = qx$. But this doesn't hold true for all substitutions of x and y.

Like at $x = 0$, $f(0,y) = 0$, which is not true. It should be $f(0,y) = y$.

For $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, the set of all solutions of $f(x,y) = 0$ be

$$\boxed{\{(x_0, y_0) \mid f(x_0, y_0) = 0\} = sol(\mathbb{K})}$$

$sol(\mathbb{K})$ can have some geometry. Like for $\{(x,y) \in \mathbb{R}^2 \mid y = x^2\}$ represents a parabola

Using change of variables for degree 3 polynomials, we can express them as

$$\boxed{y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6}$$

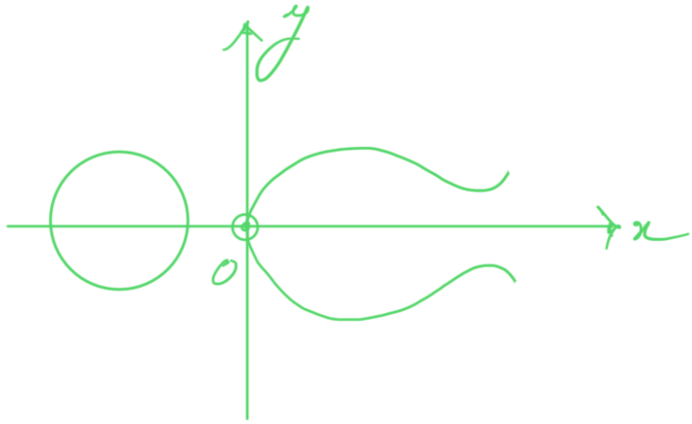
which is called the generalized Weirstrass form. If characteristic$(\mathbb{K}) \notin \{2, 3\}$, then it can be further simplified to $\boxed{y^2 = x^3 + Ax + B}$.

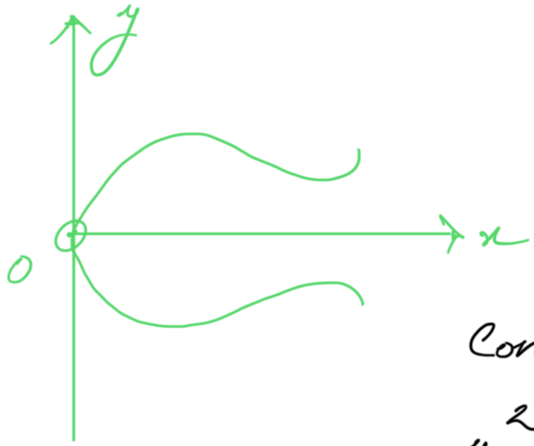
An elliptic curve over $\mathbb{K}$ has equation of the above form. It is represented by $E/\mathbb{K}$.

If $\begin{matrix}\mathbb{K}' \\ | \\ \mathbb{K}\end{matrix}$, then $E/\mathbb{K}$ and $E/\mathbb{K}'$ are different elliptic curves with the same equation.

$\boxed{\Delta = 4A^3 + 27B^2 \neq 0}$ is called the discriminant.

$E/\mathbb{R}$ typically looks like





Note that it either has 1 or 3 roots.

Consider the $E/\mathbb{R}$ $y^2 = x^3 + 2x + 3$. Take a large prime p and look at the same equation for $E/\mathbb{F}_p$ where $\begin{array}{c}\mathbb{R}\\ | \\ \mathbb{F}_p\end{array}$. The solution sets for $E/\mathbb{F}_p$ and $E/\mathbb{R}$ are going to be different since the arithmetic of $\mathbb{F}_p$ and $\mathbb{R}$ are different.

This is why we dont have a geometry for $E/\mathbb{F}_p$. We will use the intuition of $E/\mathbb{R}$ to understand $E/\mathbb{R}$. This kind of methodology is called Algeb raic Geometry.

Suppose $f(x,y)=0$ is an equation over $\mathbb{R}$. A tangent line to the graph (f) at (x_0, y_0) such that $f(x_0, y_0) = 0$, is given by

$$\boxed{T(x_0, y_0) : (y - y_0) = m\,(x - x_0)}$$ where

$$m = \left.\frac{dy}{dx}\right|_{(x_0,\, y_0)}.$$ is the slope of T.

$T(x_0, y_0)$ must be defined at every point on $E/\mathbb{R}$.

Proof/ $y^2 = x^3 + Ax + B$

$\Rightarrow y = \pm\sqrt{x^3 + Ax + B}$

When $y \neq 0$, $\dfrac{dy}{dx} = \pm \dfrac{3x^2 + A}{2\sqrt{x^3 + Ax + B}}$

For a well defined tangent line

$\dfrac{dy}{dx} = 0$ and $x^3 + Ax + B \geq 0$

For $x^3 + Ax + B = 0$, we do implicit differentiation $\frac{d}{dx}(y^2) = 3x^2 + A$

$$\Rightarrow 2y \frac{dy}{dx} = 3x^2 + A$$

$$\Rightarrow \frac{dy}{dx} = \frac{3x^2 + A}{2y}$$

When $y = 0$ but $3x^2 + A \neq 0$, interchanging x and y, the slope becomes 0. Re interchanging x and y, we get the tangent line parallel to the y axis.

When $y = 0$ and $3x^2 + A = 0$, we substitute A by $(-A)$. So $3x^2 - A = 0$

$$\Rightarrow x = \pm\sqrt{\frac{A}{3}}.$$

Using this value of x in $y^2 = x^3 - Ax + B$

$$\Rightarrow 0 = \left(\sqrt{\frac{A}{3}}\right)^3 - A\left(\sqrt{\frac{A}{3}}\right) + B$$

$$\Rightarrow \sqrt{\frac{A}{3}}\left(\frac{-2A}{3}\right) + B = 0$$

$$\Rightarrow \frac{2A^{3/2}}{3\sqrt{3}} = B$$

$$\Rightarrow 4A^3 - 27B^2 = 0$$

or $4A^3 + 27B^2 = 0$ for $x = -\sqrt{A/3}$.

$\Delta = 4A^3 + 27B^2 \neq 0$ for the tangent to be defined at every point on $E/\mathbb{R}$.

Let $\mathbb{K}$ be $\mathbb{R}$ or a field with the characteristic $\notin \{2, 3\}$. A cubic $f(x) = x^3 + Ax + B$ over $\mathbb{K}$ does not have any repeated roots in $\overline{\mathbb{K}}$ if and only if $\Delta = 4A^3 + 27B^2 \neq 0$.

Proof/ Over $\overline{\mathbb{K}}$, $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$

$$\Rightarrow \alpha_1 + \alpha_2 + \alpha_3 = 0$$

$$\alpha_1(\alpha_2 + \alpha_3) + \alpha_2\alpha_3 = A$$

$$\alpha_1\alpha_2\alpha_3 = -B$$

Suppose f has a repeated root $\alpha_1 = \alpha_2 = \alpha$.

$\Rightarrow \alpha = -2\alpha$

3

$\Rightarrow A = -3a^2$ and $B = -2a^3$

$$\Rightarrow \frac{A^3}{B^2} = -\frac{27}{4}$$

$$\Rightarrow 4A^3 + 27B^2 = \Delta = 0$$

Since $\Delta \neq 0$, we cannot have repeated roots.