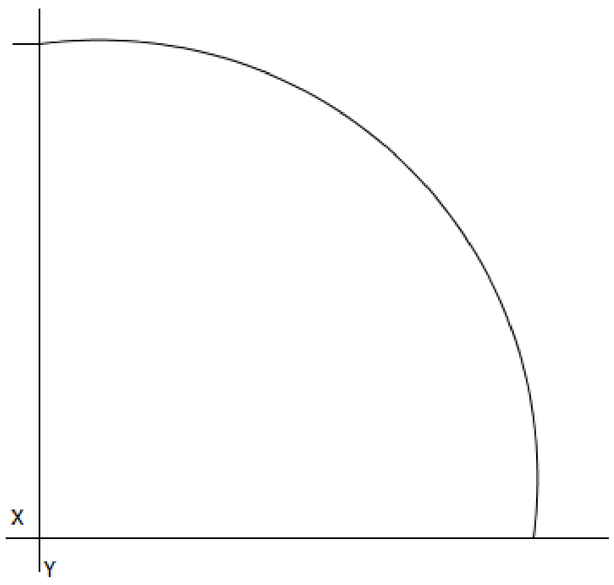
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA
DEPARTAMENTO DE MATEMÁTICA PURA E APLICADA
Curso de Licenciatura em Matemática

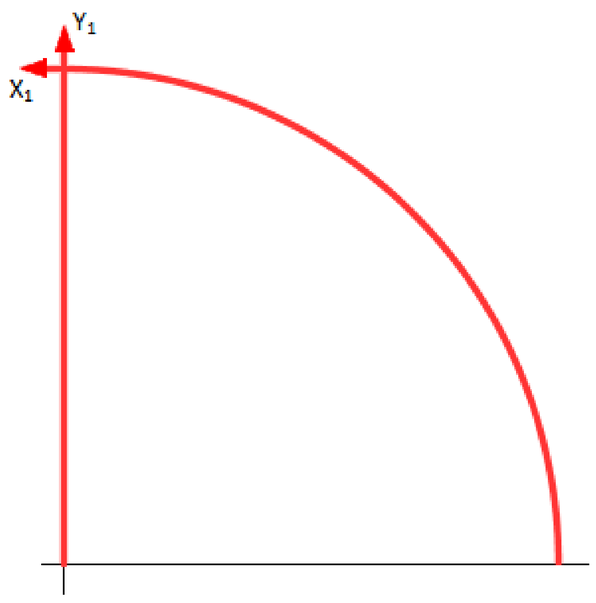
A família de curvas $y^2 - x^3 - rx = 0$

O Plano Projetivo



"Duas retas paralelas euclidianas se interceptam, no plano projetivo, em um único ponto."

Infinito Vertical



A transformação de Newton:

$$x_1 = \frac{x}{y} \qquad y_1 = \frac{1}{y}$$

Curvas elípticas

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

"As curvas elípticas formam uma estrutura de grupo."

A família de curvas $y^2 - x^3 - rx = 0$ é um caso particular de curva elíptica.
Usando a transformação de Newton ela fica da forma: $y_1 = x_1^3 + r\,x_1\,y_1^2$.

Operação do grupo das curvas elípticas

Dados dois pontos P e Q de uma curva elíptica *C*.

1. Encontrar a reta *r* determinada por P e Q, caso P e Q não sejam pontos distintos basta tomar a reta tangente à curva *C* no ponto P.
2. Encontrar o ponto I de interseção entre a reta *r* e a curva *C*.
3. Traçar a reta *s* paralela ao eixo das ordenadas que passa por I.
4. Sabemos que a reta *s* intercepta o eixo das ordenadas em um único ponto, o ponto de origem do infinito vertical.
5. Temos que P + Q é o primeiro ponto de interseção entre a reta *s* e a curva *C* quando prolongamos a reta *s* ao infinito.

Objetivo do Trabalho

1. Tomamos a curva de Billing: $y^2 = x_1^3 - 82\,x_1$.
2. Usamos a transformação de Newton para trabalhar no infinito vertical e obtemos: $y_1 = x_1^3 - 82\,x_1\,y_1^2$, uma cúbica de Chasles.
3. Descrevemos a operação do grupo das curvas elípticas nas cúbicas de Chasles.
4. Observamos casos da associatividade dessa operação.

Autora: Graziela Langone Fonseca
Orientador: Dr. Alexandre Tavares Baraviera