Universidade Federal de Minas Gerais

Departamento de Matemática

O Teorema de Mordell

Wodson Mendson

Sejam $a, b \in \mathbb{Z}$ e considere $f(X, Z) = X^3 + aXZ^2 + bZ^3 \in \mathbb{Z}[X, Z]$. Suponha que f é não singular. Para simplificar a exposição iremos supor que $f(X, Z) = (X - a_1Z)(X - a_2Z)(X - a_3Z)$ com $a_1, a_2, a_3 \in \mathbb{Z}$. Em particular, temos $a_i \neq a_j$ se $i \neq j$.

Seja $F(X, Y, Z) = ZY^2 - f(X, Z) \in \mathbb{Z}[X, Y, Z]$ e considere o seguinte conjunto:

$$X_F(\mathbb{Q}) := \{[x : y : z] \in \mathbb{P}^2_{\mathbb{Q}} \mid F(x, y, z) = 0\}.$$

$X_F(\mathbb{Q})$ descreve uma curva projetiva sobre $\mathbb{Q}$. Denote $\mathcal{O} = [0 : 1 : 0]$. Chamaremos tal ponto de **ponto no infinito** da cúbica descrita por F. Observe que se $P = [u : v : t] \in X_F(\mathbb{Q})$ é tal que $P \neq \mathcal{O}$ então $t \neq 0$. Assim, existe uma bijeção

$$X_F(\mathbb{Q}) \cong \{(u, v) \in \mathbb{Q}^2 \mid F(u, v, 1) = 0\} \cup \{\mathcal{O}\}.$$

Dessa forma, podemos encarar o conjunto $X_F(\mathbb{Q})$ como uma curva afim descrita por $g(X, Y) = Y^2 - f(X, 1)$ munida de um ponto "extra".

1 A estrutura de grupo

No que se segue fixamos $a, b \in \mathbb{Z}$ e consideramos o conjunto $X_F(\mathbb{Q})$ tal como definido acima.

Definição 1. *O mapa multiplicação em $X_F(\mathbb{Q})$, denotado por $*$, associa $(P, Q) \in X_F(\mathbb{Q})^2 \mapsto P * Q$ é definido da seguinte forma:*

Tome L a reta passando por P e Q. Pelo teorema de Bezout, sabemos que L intersecta $X_F(\mathbb{C})$ em um terceiro ponto R. Como as operações envolvidas para calcular R são realizadas sobre o corpo primo $\mathbb{Q}$, temos que R possui coeficientes em $\mathbb{Q}$ i.e. $R \in X_F(\mathbb{Q})$. Definimos $P * Q := R$.

A seguinte proposição estabelece algumas propriedade da operação $*$.

Proposição 1. *A operação $*$ satisfaz as seguintes propriedades:*

(i) $P * Q = Q * P$

(ii) $P * (P * Q) = Q$.

(iii) $P * P = P$ *se e somente se* P *é um ponto de inflexão.*

(iv) $\mathcal{O} * \mathcal{O} = \mathcal{O}$.

Demonstração. Os itens (i) e (ii) são triviais. O item (iii) segue da definição de ponto de inflexão. Relembre que $P \in X_F(\mathbb{C})$ é dito um ponto de inflexão se $L \cap X_F(\mathbb{C}) = \{P\}$, onde L denota a reta tangente a $X_F(\mathbb{Q})$ sobre P. Uma verificação rotineira, mostra que $\mathcal{O}$ é um ponto de inflexão.

□

Exercício 1. *Verifique que a operação $*$ não estabelece uma lei de grupo no conjunto $X_F(\mathbb{Q})$.*

Agora, vamos equipar o conjunto $X_F(\mathbb{Q})$ com uma lei de grupo. Para esse fim, fixaremos $\mathcal{O} = [0 : 1 : 0]$ e usaremos tal ponto para desempenhar o elemento neutro.

Definição 2. *Sejam $P, Q \in X_F(\mathbb{Q})$. A operação soma $+$ em $X_F(\mathbb{Q})$ é definida pondo*

$$P + Q := \mathcal{O} * (P * Q).$$

Teorema. *$(X_F(\mathbb{Q}), +)$ é um grupo abeliano com $\mathcal{O}$ desempenhando o elemento neutro.*

Demonstração. Seja $P \in X_F(\mathbb{Q})$. Temos que $P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = \mathcal{O} * (\mathcal{O} * P) = P$. Além disso, se $Q = \mathcal{O} * P$ temos $P + Q = \mathcal{O} * (P * (\mathcal{O} * P)) = \mathcal{O} * \mathcal{O} = \mathcal{O}$ por (iv) da proposição acima. Assim, temos a fórmula para o inverso $-P = \mathcal{O} * P$. Resta verificar a associatividade. Para isso, devemos provar que dados $P, Q, R \in X_F(\mathbb{Q})$ temos $(P + Q) + R = P + (Q + R)$. Ora, por definição

$$(P + Q) + R = \mathcal{O} * (R * (\mathcal{O} * (P * Q))) \qquad P + (Q + R) = \mathcal{O} * (P * (\mathcal{O} * (R * Q))).$$

Aplicando $\mathcal{O}$ vemos que é suficiente mostrar a seguinte igualdade

$$R * (\mathcal{O} * (P * Q)) = P * (\mathcal{O} * (R * Q)).$$

Isso pode ser provado por computação tediosa, o qual omitimos.

□

Exercício 2. *Seja $P = [x : y : 1] \in X_F(\mathbb{Q})$. Verifique que $-P = [x : -y : 1]$.*

Proposição 2. *Sejam $P, Q, R \in X_F(\mathbb{Q})$.*

$$P + Q + R = \mathcal{O} \iff P, Q \text{ e } R \text{ são colineares.}$$

Demonstração.

$$P + Q + R = \mathcal{O} \iff \mathcal{O} * (R * (\mathcal{O} * (P * Q))) = \mathcal{O} \iff R = \mathcal{O} * (\mathcal{O} * (P * Q)) = P * Q.$$

□

Corolário 1. *$3P = \mathcal{O}$ se e só se P é um ponto de inflexão.*

Demonstração. Pela proposição acima, $P + P + P = \mathcal{O}$ se e só a reta tangente sobre P tem contato triplo com $X_F(\mathbb{C})$.

□

2 Grupos normados

Seja G um grupo abeliano (notação aditiva). Observe que para cada $n \in \mathbb{N}$ obtemos um mapa de grupos

$$[n] : G \longrightarrow G \qquad g \mapsto ng.$$

onde $Ker([n]) = G[n]$, $Im([n]) = nG$ e $Coker([n]) = G/nG$.

Denotamos $[G : nG] = \#Coker([n])$. Dizemos que nG é de indice finito em G se $[G : nG] < \infty$. Note que se G é finitamente gerado então $[G : nG] < \infty$. Nessa seção, mostramos a reciproca para uma classe particular de grupos. Mais precisamente, mostraremos que se G é um grupo abeliano normado com $[G : 2G] < \infty$ então G é finitamente gerado.

Definição 3. *Seja G um grupo abeliano. Dizemos que G é normado se existir uma função $h : G \longrightarrow \mathbb{R}_{\geq 0}$ tal que:*

(i) Para cada $r \in \mathbb{R}_{\geq 0}$ o conjunto $H(r) := \{P \in G \mid h(P) \leq r\}$ é finito.

(ii) $h(mP) = |m|^2 h(P)$ para todo $P \in G$ e $m \in \mathbb{Z}$.

(iii) $h(P + Q) + h(P - Q) = 2h(P) + 2h(Q)$ (regra do paralelogramo).

Uma função satisfazendo as propriedades acima é dita uma ***função altura em*** *G. Dizemos que G é normado se pode ser equipado com uma função altura.*

Observação 1. *Suponha que G é um grupo munido de uma função altura h e denote por $G_{tor} := \{g \in G \mid ng = 0\}$ por algum $n \in \mathbb{Z}$. Nesse caso, temos que $\#G_{tor} < \infty$. De fato, note que $ng = 0$ implica que $0 = h(0) = h(ng) = |n|h(g) \Longrightarrow h(g) = 0$. Assim, $G_{tor} \subseteq H(0)$ e por (i) temos $\#H(0) \leq \infty$.*

Exemplo 1. *Seja $\mathbb{R}^n$ com a norma euclidiana $|\ \ |$ e considere a função $h : \mathbb{Z}^n \longrightarrow \mathbb{R}_{\geq 0}$ que associa $P \mapsto h(P) := |P|^2 = < P, Q >$, a restrição do produto interno usual de $\mathbb{R}^n$ em $\mathbb{Z}^n$. Então, h é uma função altura em $G := \mathbb{Z}^n$.*

Exemplo 2. *Seja $G_1, ..., G_r$ grupo abelianos munidos de funções alturas $h_i : G_i \longrightarrow \mathbb{R}$. Então $G := G_1 \oplus \cdots \oplus G_r$ é um grupo abeliano munido de uma função altura. De fato, defina $h : G \longrightarrow \mathbb{R}$ pondo $h(P_1 + \cdots + P_r) := h_1(P_1) + \cdots + h_r(P_r)$. Em particular, se G é finitamente gerado temos $G = G_{tor} \oplus \mathbb{Z}^r$ e assim G pode ser equipado com uma função altura.*

Teorema. *Seja G um grupo abeliano. Suponha que G é normado e $[G : 2G] < \infty$. Então G é finitamente gerado.*

Demonstração. Se G é um grupo de tipo finito, as observações acima mostram que $[G : nG] < \infty$ para todo inteiro $n > 1$ e G é normado. Reciprocamente, suponha que G é um grupo abeliano normado, com altura h, e $[G : 2G] < \infty$. Devemos mostrar que G é de tipo finito. Seja $G/2G = \{\overline{P}_1, ..., \overline{P}_k\}$ e denote por $\alpha := \mathbf{Max}\{h(P_1), ..., h(P_k)\} + 1$. Por propriedade (i) de função altura, temos que $H(\alpha)$ é um conjunto finito. Seja $S := (H(\alpha))$ o subgrupo gerado pelos pontos de $H(\alpha)$. Vamos mostrar que $G = S$.

Suponha que tal não ocorra i.e. seja $P \in G - S$. Seja $\beta := h(P)$ e tome $R \in H(\beta) \cap (G - S)$ com $h(R) \leq h(P)$ para todo $P \in H(\beta)$. Isso mostra que podemos supor que P é um elemento que não está em S e possui altura minimal com respeito a essa propriedade. Temos $\overline{P} = \overline{P}_j$ por algum j. Assim, $P = P_j + 2Q$ por algum $Q \in G$. Dai, $2Q = P_j - P$ e

$$4h(Q) = h(2Q) = h(P_j - P) = 2h(P_j) + 2h(P) - h(P_j + P) \leq 2\alpha + 2h(P) + 0.$$

Assim, $4h(Q) \leq 2\alpha + 2h(P) < 2h(P) + 2h(P) = 4h(P) \Longrightarrow h(Q) < h(P)$.

Minimalidade de P implica que $Q \in S$. Como $P_j \in S$ temos $P = P_j + 2G \in S$, o que é um absurdo. Isso demonstra o teorema.

□

3 Finitude de $[X_F(\mathbb{Q}) : 2X_F(\mathbb{Q})]$.

Relembre as convenções: $X_F(\mathbb{Q}) := \{[x : y : z] \in \mathbb{P}^2_{\mathbb{Q}} \mid F(x, y, z) = 0\}$ onde $F = ZY^2 - f(X, Z)$ com $f(X, Z) = (X - a_1Z)(X - a_2Z)(X - a_3Z)$ e $a_i \neq a_j$ se $i \neq j$ equipado com a lei de grupo descrita na 1º seção.

Nessa seção mostraremos a finitude do indice $[X_F(\mathbb{Q}) : 2X_F(\mathbb{Q})]$. Começamos provando o seguinte[1].

Critério para Divisibilidade por 2 . *Seja $(x_1, y_1) \in X_F(\mathbb{Q})$. Existe $(x_2, y_2) \in X_F(\mathbb{Q})$ tal que $2(x_2, y_2) = (x_1, y_1)$ se e somente se $x_1 - a_1, x_1 - a_2, x_1 - a_3 \in \mathbb{Q}^{*^2}$.*

Demonstração. Mostraremos apenas a implicação $\Longrightarrow$. Para mais detalhes, veja o livro do Knapp. Assim, suponha $P = (x_1, y_1)$ tal que $2(x_2, y_2) = P$. Tome L a reta passando por $-P$ e $2(x_2, y_2)$, digamos $y = mx+b$. Substituindo na equação da cubica obtemos

$$(mx + b)^2 = (x - a_1)(x - a_2)(x - a_3).$$

Por hipótese, $f(X) = (mX + b)^2 - (X - a_1)(X - a_2)(X - a_3)$ é um polinomio com raizes x_1, x_2, onde x_2 é uma raiz dupla. Assim, $f(X) = (X - x_2)^2(X - x_1)$. Avaliando em a_i, obtemos

$$(ma_i + b)^2 = (a_i - x_2)^2(a_i - x_1) \Longrightarrow (x_1 - a_i) \in \mathbb{Q}^{*^2}.$$

Assim, $x_1 - a_1, x_1 - a_2, x_1 - a_3 \in \mathbb{Q}^{*^2}$.

□

[1]Relembre a bijeção: $X_F(\mathbb{Q}) \cong \{(u, v) \in \mathbb{Q}^2 \mid y^2 = (x-a_1)(x-a_2)(x-a_3)\} \cup \{\mathcal{O}\}$ $\quad [x : y : t] \mapsto (x/t, y/t)$ se $[x : y : t] \neq \mathcal{O}$.

Proposição 3. *Defina o mapa*

$$\Phi_{a_1} : X_F(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*^2}.$$

$$P \longmapsto \begin{cases} (x-a_1)\mathbb{Q}^{*^2} & se \quad P=(x,y) \notin \{(a_1,0),\mathcal{O}\}. \\ (a_1-a_2)(a_1-a_3)\mathbb{Q}^{*^2} & se \quad P=(a_1,0). \\ 1 & se \quad P=\mathcal{O}. \end{cases}$$

Então, Φ_{a_1} é um mapa de grupos.

Assim, como $\Phi_{a_1}(2P) = \Phi_{a_1}(P)^2 = 1 \mod \mathbb{Q}^*$ temos que $2X_F(\mathbb{Q}) \subset Ker(\Phi_{a_1})$ de modo que Φ_{a_1} induz $\varphi_{a_1} : X_F(\mathbb{Q})/2X_F(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*^2}$, por passagem ao quociente.

Demonstração. Sejam $P_1, P_2, P_3 \in X_F(\mathbb{Q})$. Note que para mostrar que Φ_{a_1} é um mapa de grupos é suficiente mostrar que

$$P_1 + P_2 + P_3 = \mathcal{O} \Longrightarrow \Phi_{a_1}(P_1)\Phi_{a_1}(P_2)\Phi_{a_1}(P_3) = 1.$$

Observe que se $P_i = \mathcal{O}$ por algum i, então o resultado é trivial. Assim, suporemos $P_1, P_2, P_3 \neq \mathcal{O}$.

1º Caso: $P_1, P_2, P_3 \neq (a_1, 0)$. Nesse caso, tome $L : Y = mX + b$ a reta passando por P_1, P_2 e P_3. Então x_1, x_2 e x_3 são raizes do polinômio $f(X) = (mX+b)^2 - (X-a_1)(X-a_2)(X-a_3)$. Assim, $f(X) = (X-x_1)(X-x_2)(X-x_3)$. Tomando $X = x_1$, obtemos

$$(x_1-a_1)(x_1-a_2)(x_1-a_3) = (mx_1+b)^2 \in \mathbb{Q}^{*^2}.$$

Dai, $(x_1-a_1)(x_1-a_2)(x_1-a_3) = \Phi_{a_1}(P_1)\Phi_{a_1}(P_2)\Phi_{a_1}(P_3) = 1$ em $\mathbb{Q}^*/\mathbb{Q}^{*^2}$.

2º Caso: $P_1 = (a_1, 0)$. Temos assim que $P_2, P_3 \neq (a_1, 0)$. Seja $L : Y = mX + b$ a reta passando por P_1, P_2, P_3. Então, a_1, x_2, x_3 são raizes do polinomio $f(X) = (mX+b)^2 - (X-a_1)(X-a_2)(X-a_3)$ i.e. $(mX+b)^2 - (X-a_1)(X-a_2)(X-a_3) = (X-a_1)(X-x_2)(X-x_3)$. Em particular, $X - a_1$ divide $mX + b \Longrightarrow mX + b = d(X-a_1)^2$, com $d \in \mathbb{Q}$. Fazendo as devidas simplificações obtemos

$$d(X-a_1) - (X-a_2)(X-a_3) = (X-x_2)(X-x_3).$$

Avaliando em $X = a_1$ obtemos $(a_1-a_2)(a_1-a_3) = (a_1-x_2)(a_1-x_3)$ e assim $\Phi_{a_1}(P_1) = \Phi_{a_1}(P_2)\Phi_{a_2}(P_3) \Longrightarrow \Phi_{a_1}(P_1)\Phi_{a_1}(P_2)\Phi_{a_2}(P_3) = 1$.

□

De maneira análoga podemos considerar o mapa Φ_{a_2}. Assim, tomando o produto, obtemos o mapa:

$$\Phi_{a_1} \times \Phi_{a_2} : X_F(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*^2} \times \mathbb{Q}^*/\mathbb{Q}^{*^2}.$$

Proposição 4. $Ker(\Phi_{a_1} \times \Phi_{a_2}) = 2X_F(\mathbb{Q})$.

Demonstração. Pela proposição acima temos $2X_F(\mathbb{Q}) \subset Ker(\Phi_{a_1} \times \Phi_{a_2})$. Agora, seja $P = (x, y) \in Ker(\Phi_{a_1} \times \Phi_{a_2})$. Considere os casos:

1º Caso: $P \notin \{(a_1, 0), (a_2, 0)\}$**.** Nesse caso, temos que $x - a_1, x - a_2 \in \mathbb{Q}^{*^2}$. Da equação $y^2 = (x-a_1)(x-a_2)(x-a_3)$ obtemos $x - a_3 \in \mathbb{Q}^{*^2}$ e pelo critério de divisibilidade por 2 temos que existe $(x_2, y_2) \in X_F(\mathbb{Q})$ tal que $2(x_2, y_2) = (x_1, y_1)$.

2º Caso: $P = (a_1, 0)$**.** Nesse caso, temos $(a_1 - a_2)(a_1 - a_3) \in \mathbb{Q}^{*^2}$ e $(a_1 - a_2) \in \mathbb{Q}^{*^2}$. Dai, $(a_1 - a_3) \in \mathbb{Q}^{*^2}$. Como 0 é quadrado, $a_1 - a_2$ e $a_1 - a_3$ são quadrados, segue do critério de divisibilidade que $(a_1, 0) = 2(x_2, y_2)$ para algum $(x_2, y_2) \in X_F(\mathbb{Q})$.

3º Caso: $P = (a_2, 0)$**.** Inteiramente análogo ao caso anterior.

□

Assim, obtemos um mapa injetivo

$$\varphi_{a_1} \times \varphi_{a_2} : X_F(\mathbb{Q})/2X_F(\mathbb{Q}) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*^2} \times \mathbb{Q}^*/\mathbb{Q}^{*^2}.$$

Para provar o próximo teorema usaremos a **função p-ádica:**

Definição 4. *Seja $p \in \mathbb{Z}$ um primo. Seja $n = a/b \in \mathbb{Q}$ uma fração reduzida i.e. $mdc(a, b) = 1$. Escreva $n = p^{\alpha} a^{'}/b^{'}$, onde $mdc(a^{'}, p) = mdc(b^{'}, p) = 1$. Definimos $ord_p(n) := \alpha$. Por convenção, definimos $ord_p(0) = \infty$.*

Observe que se $n \in \mathbb{Z}$ então $ord_p(n)$ é o expoente do inteiro primo p ocorrendo na decomposição de n.

Proposição 5. *A função ord_p satisfaz as seguintes proprieades:*

*(i) $\forall\, n, m \in \mathbb{Q}$ temos $ord_p(n+m) \geq$ **Min**$(ord_p(n), ord_p(m))$ com igualdade se e só se $ord_p(n) \neq ord_p(m)$*

(ii) $ord_p(nm) = ord_p(n) + ord_p(m)$.

Demonstração. um exercicio simples.

□

No que se segue usaremos a bijeção:

$$f : \mathbb{Q}^*/\mathbb{Q}^{*^2} \longrightarrow \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_{p \in \mathbb{Z} \text{ primo}} \mathbb{Z}/2\mathbb{Z}$$

que associa $\alpha = \overline{(-1)^{a_0} p_1^{a_1} \cdots p_k^{a_k}} \mapsto (a_0 \mod 2, a_1 \mod 2, ..., a_k \mod 2)$. Por meio de tal identificação, diremos a $a_j \mod 2$ é a p_j-ésima componente de α.

O próximo teorema garante que $[X_F(\mathbb{Q}) : 2X_F(\mathbb{Q})] < +\infty$.

Teorema. *Seja $f(X) = (X - a_1)(X - a_2)(X - a_3)$ e $D := \prod_{i<j}(a_i - a_j)^2$. Seja $|D| = \prod_k p_k^{l_k}$ a decomposição em fatores primos. Então,*

$$Im(\varphi_{a_1} \times \varphi_{a_2}) \subset \{((-1)^{t_{01}} p_1^{t_{11}} \cdots p_r^{t_{r1}}, (-1)^{t_{02}} p_1^{t_{12}} \cdots p_r^{t_{r2}}) \mid t_{ij} \in \{0, 1\}\}.$$

Em particular, $[X_F(\mathbb{Q}) : 2X_F(\mathbb{Q})] < +\infty$.

Demonstração. Seja $P = (x, y) \in X_F(\mathbb{Q})$ e defina $S := \{((-1)^{t_{01}} p_1^{t_{11}} \cdots p_r^{t_{r1}}, (-1)^{t_{02}} p_1^{t_{12}} \cdots p_r^{t_{r2}}) \mid t_{ij} \in \{0, 1\}\}$. Vamos mostrar que

$$\Phi_{a_1} \times \Phi_{a_2}(P) \in S.$$

Consideremos dois casos:

1º Caso $x \notin \{a_1, a_2, a_3\}$**:** Nesse caso, fixe um primo $p \in \mathbb{Z}$ e defina A, B e $C \in \mathbb{Z}$ pondo

$$A := ord_p(x - a_1) \qquad B := ord_p(x - a_2) \qquad C := ord_p(x - a_3).$$

Pela equação da cúbica, sabemos que $y^2 = (x-a_1)(x-a_2)(x-a_3)$. Dai, pela propriedade (ii) da função ord_p temos que

$$2ord_p(y) = ord_p((x-a_1)(x-a_2)(x-a_3)) = ord_p(x-a_1) + ord_p(x-a_2) + ord_p(x-a_3) = A+B+C.$$

Em particular, $A+B+C \equiv 0 \mod 2$. Observe que se $A=B=C=0$ então $\Phi_{a_1}(P) = (x-a_1)\mathbb{Q}^{*^2} = 1$ e $\Phi_{a_2}(P) = (x-a_2)\mathbb{Q}^{*^2} = 1$ de modo que $(\Phi_{a_1} \times \Phi_{a_2})(P) = (1,1) \in S$. Suponha que ao menos um dos inteiros A, B e C é negativo, digamos $A < 0$. Então, como $a_1 \in \mathbb{Z}$ sabemos que $A = ord_p(x-a_1) = ord_p(x)$ (aplique propriedade (i) da função ord_p). Assim, $B = ord_p(x-a_2) = ord_p(x)$ e $C = ord_p(x-a_3) = ord_p(x)$ de modo que $A = B = C$. Pelo fato, $A+B+C \equiv 0 \mod 2$ obtemos $A \equiv 0$, $B \equiv 0$, $C \equiv 0 \mod 2$. Assim, a p-ésima componente de $\Phi_{a_1}(P)$ e $\Phi_{a_2}(P)$ é 0.

Suponha agora que ao menos um dos inteiros A, B e C é positivo, digamos $A > 0$. Temos,

$$B = ord_p(x-a_2) = ord_p((x-a_1)+(a_1-a_2)) \geq \mathbf{Min}(ord_p(x-a_1), ord_p(a_2-a_1)) = \mathbf{Min}(A, ord_p(a_2-a_1)).$$

Assuma que p não divide $|D|$. Nesse caso, $A > 0 = ord_p(a_2-a_1)$ e por propriedade (i) da função ord_p temos que $B = \mathbf{Min}(A, ord_p(a_2-a_1)) = 0$. Analogamente, temos que $C = 0$. Assim, usando o fato $A+B+C = A \equiv 0 \mod 2$ concluimos que A é par. Assim, a p-ésima componente de $\Phi_{a_1}(P)$ e $\Phi_{a_2}(P)$ vale 0.

2º Caso $x \in \{a_1, a_2, a_3\}$**:** Nesse caso, $\Phi_{a_i}(P)$ é da forma $(a_k - a_j)\mathbb{Q}^{*^2}$. Assim, se p não divide $|D|$ temos que $ord_p((a_k-a_j)) = 0$ de modo que a p-ésima componente é nula.

Conclusão: Os únicos primos que possivelmente ocorrem em $\Phi_{a_1}(P)$ e $\Phi_{a_2}(P)$ são aqueles que dividem o discriminante $|D|$. Assim, $\Phi_{a_1} \times \Phi_{a_2}(P) \in S$.

□

4 Função altura no grupo $X_F(\mathbb{Q})$

Nessa seção, construimos uma função altura no grupo $X_F(\mathbb{Q})$.

Definição 5. *Seja $a/b \in \mathbb{Q}$ escrito na forma reduzida. Definimos a pseudo-altura de a/b pondo $H(a/b) :=$ **Max**$(|a|,|b|)$. A altura logaritmica é definida tomando o logaritmo; $h(a/b) := log(H(a/b))$.*

Observe que para cada $n \in \mathbb{R}$ o conjunto $\{\alpha \in \mathbb{Q} \mid h(\alpha) < n\}$ é finito, já que existe um número finito de naturais m tais que $m < n$.

Definição 6. *Seja $P \in X_F(\mathbb{Q})$. Se $P \neq \mathcal{O}$ escreva $P = [x : y : 1]$. A função **altura logaritmica** em $X_F(\mathbb{Q})$é definida pondo*

$$\tilde{h}(\mathcal{O}) = 0 \quad e \quad \tilde{h}(P) = h(x).$$

Observação 2. *Dado $n \in \mathbb{R}$ o conjunto*

$$\{P \in X_F(\mathbb{Q}) \mid \tilde{h}(P) < n\}$$

é finito.

Definição 7. *Sejam G um grupo abeliano e $f : G \longrightarrow \mathbb{R}_{\geq 0}$ uma aplicação. Diremos que f é discreta se para qualquer $r \in \mathbb{R}$, o conjunto*

$$\{\alpha \in G \mid f(\alpha) < r\}$$

é finito.

Pela observação acima, concluimos que a função altura logaritmica em $X_F(\mathbb{Q})$ é discreta.

Lema 1. *Existe uma constante $c \in \mathbb{R}_{\geq 0}$ tal que para quaisquer $P, Q \in X_F(\mathbb{Q})$ temos*

$$|\tilde{h}(P+Q) + \tilde{h}(P-Q) - 2\tilde{h}(P) - 2\tilde{h}(Q)| \leq c$$

Demonstração. Veja [1], pág 218 ou exercicio 3.2 de [2] na pág 102. □

Teorema. *Seja X uma curva eliptica sobre* [2] *$\mathbb{Q}$. Existe uma função*

$$\sigma : X_F(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}.$$

que possui as seguintes propriedades:

(i) $\sigma(P) \geq 0$ para todo $P \in X_F(\mathbb{Q})$.

(ii) Existe uma constante $r \in \mathbb{R}_{\geq 0}$ tal que

$$|\sigma(P) - \frac{1}{2}\tilde{h}(P)| < r.$$

(iii) σ é discreta.

(iv) $\sigma(mP) = m^2\sigma(P)$ para todo $P \in X_F(\mathbb{Q})$.

(v) $\sigma(P+Q) + \sigma(P-Q) = 2\sigma(P) + 2\sigma(Q)$ para todos pontos $P, Q \in X_F(\mathbb{Q})$.

(vi) $\sigma(P) \neq 0$ se e só se $P \notin X_F(\mathbb{Q})_{tor}$.

Demonstração. Usando o lema acima com $P = Q$, obtemos

$$|\tilde{h}(2P) - 4\tilde{h}(P)| < c \quad \text{para todo } P \in X_F(\mathbb{Q}).$$

Defina

$$\delta(P) := \lim_{n\to\infty} \frac{\tilde{h}(2^n P)}{4^n} \quad \text{e} \quad \sigma(P) := \frac{1}{2}\delta(P).$$

Obseve que o limite acima existe. Com efeito, temos

$$\frac{\tilde{h}(2^n P)}{4^n} = \tilde{h}(P) + \sum_{k=1}^{n} \frac{1}{4^k}(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P)) \qquad (*).$$

Agora,

$$\frac{1}{4^k}|(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P))| < \frac{1}{4^k}c.$$

Assim, por teste de comparação, a série $\sum_{k=1}^{n} \frac{1}{4^k}(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P))$ converge de modo que o limite

$$\lim_{n\to\infty} \frac{\tilde{h}(2^n P)}{4^n} = \tilde{h}(P) + \sum_{k=1}^{\infty} \frac{1}{4^k}(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P))$$

existe.

[2] lembre das convenções.

(i): Se segue da definição da função δ.

(ii) Temos

$$|\sigma(P) - \frac{1}{2}\tilde{h}(P)| = |\frac{1}{2}\delta(P) - \frac{1}{2}\tilde{h}(P)| = \frac{1}{2}|\delta(P) - \tilde{h}(P)|.$$

Assim, por $(*)$ obtemos

$$|\delta(P) - \tilde{h}(P)| \leq |\sum_{k=1}^{\infty} \frac{1}{4^k}(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P))| \leq \sum_{k=1}^{\infty} \frac{1}{4^k}|(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P))| < \sum_{k=1}^{n} \frac{1}{4^k} c = \frac{c}{3}$$

de modo que

$$|\sigma(P) - \frac{1}{2}\tilde{h}(P)| < \frac{c}{6} \qquad (**)$$

(iii) Seuponha que $\sigma(P) < r$, por algum $r \in \mathbb{R}$. Usando $(**)$ temos $\frac{1}{2}\tilde{h}(P) < \sigma(P) + \frac{c}{6} < r + \frac{c}{6}$. Assim, a função σ é discreta já que $\tilde{h}$ é discreta.

(v) Usando o lema técnico temos

$$\frac{1}{4^n}|\tilde{h}(2^n(P+Q)) + \tilde{h}(2^n(P-Q)) - 2\tilde{h}(2^n P) - 2\tilde{h}(2^n Q)| < \frac{c}{4^n}.$$

Por passagem ao limite obtemos a regra do paralelogramo $\sigma(P+Q) + \sigma(P-Q) = 2\sigma(P) + 2\sigma(Q)$.

(iv) Isso se segue por indução em m. Para $m = 2$ temos

$$\delta(2P) = \lim_{k\to\infty} \frac{1}{4^k}\tilde{h}(2^{k+1}P) = 4 \lim_{k\to\infty} \frac{1}{4^{k+1}}\tilde{h}(2^{k+1}P) = 4\delta(P).$$

Assim, $\sigma(2P) = 4\sigma(P)$. Para o caso geral seja $m \in \mathbb{N}$. Então,

$$\sigma((m+1)P) = \sigma(mP + P) = 2\sigma(mP) + 2\sigma(P) - \sigma((m-1)P) \qquad \text{pela regra do paralelogramo.}$$

Dai, pela hipótese de indução vem $2\sigma(mP)+2\sigma(P)-\sigma((m-1)P) = 2m^2\sigma(P)+2\sigma(P)-(m-1)^2\sigma(P) = (2m^2 + 2 - m^2 + 2m - 1)\sigma(P) = (m^2 + 2m + 1)\sigma(P) = (m+1)^2\sigma(P)$.

(iv) Seja $P \in X_F(\mathbb{Q})_{tor}$. Então, $nP = \mathcal{O}$ por algum $n > 1$. Temos assim, $0 = \sigma(nP) = n^2\sigma(P) \Longrightarrow \sigma(P) = 0$. Suponha que $\sigma(P) = 0$. Considere o conjunto $S := \{nP \mid n \in \mathbb{N}\}$. Como $S \subset \{P \in X_F(\mathbb{Q}) \mid h(Q) = 0\}$ e a função σ é discreta, temos que S é finito. Em particular, P tem ordem finita.

□

Corolário 2. *A função σ ocorrendo no teorema acima define uma norma no grupo $X_F(\mathbb{Q})$.*

Assim, combinando os resultados obtidos com os resultados das seções anteriores obtemos o seguinte

Teorema (Mordell -1922). *$(X_F(\mathbb{Q}), +)$ é um grupo abeliano finitamente gerado.*

5 Referências

[1] Washington, Lawrence C. Elliptic curves: number theory and cryptography. CRC press, 2008.

[2] Silverman, J. H., Tate, J. T. (1992). Rational points on elliptic curves (Vol. 9). New York: Springer-Verlag.

[3] Knapp, A. W. (1992). Elliptic curves (Vol. 40). Princeton University Press.