Curvas Elípticas com Multiplicação Complexa

Aluno: Adrian Alexander Ticona Delgado
Orientador: Kostiantyn Iusenko

IME - USP
2021

O conteúdo está dividido em cinco partes

- PARTE I - Introdução e Motivação
- PARTE II - Superfícies de Riemann e Curvas Algébricas
- PARTE III - Curvas Elípticas
- PARTE IV - Teoria Algébrica dos Números - CFT Global
- PARTE V - Multiplicação Complexa

PARTE I - Introdução e Motivação

K - corpo de números algébricos (i.e. $K/\mathbb{Q}$ finito)

L/K abeliano : L/K Galois com $\mathrm{Gal}(L/K)$ abeliano

PARTE I - Introdução e Motivação

K - corpo de números algébricos (i.e. $K/\mathbb{Q}$ finito)

L/K abeliano : L/K Galois com $Gal(L/K)$ abeliano

Quando $K = \mathbb{Q}$, uma descrição de todas as suas extensões abelianas é fornecida pelo

Teorema de Kronecker-Weber

$e^{\frac{2\pi i}{n}}$

Se $L/\mathbb{Q}$ é finita e abeliana, então $L \subseteq \mathbb{Q}(\zeta_n)$ para algum $n \geq 1$ ($\mathbb{Q}(\zeta_n)$: n-ésimo corpo ciclotômico)

" $\mathbb{Q}(\zeta_n)$: n-ésimo corpo ciclotômico "

Tais extensões são obtidas a partir de raízes da unidade que são precisamente os pontos de torção dos pontos complexos de $\mathbb{G}_m = \{(x,y) : xy = 1\}$ $\left(\mathbb{G}_m(k) \text{ "}=\text{" } k^*\right)$

" $\mathbb{Q}(\zeta_n)$: n-ésimo corpo ciclotômico "

Tais extensões são obtidas a partir de raízes da unidade que são precisamente os pontos de torção dos pontos complexos de $\mathbb{G}_m = \{(x,y) : xy = 1\}$ $(\mathbb{G}_m(k) \text{ "}=\text{" } k^*)$

Exemplo: $\mathbb{G}_m(\mathbb{C}) = \mathbb{C}^*$ e $\zeta = e^{\frac{2\pi i}{5}}$ tem ordem 5

O que vamos mostrar é que podemos obter algo semelhante para K corpo quadrático imaginário (i.e. $K \not\subseteq \mathbb{R}$).

PARTE II - Superfícies de Riemann e Curvas Algébricas

DEF: X localmente homeomorfo a um aberto de $\mathbb{C}$ com cartas holomorfas

$X = S^2$

$X \subseteq \mathbb{P}^n$ dado pelo anulamento de polinómios homogéneos / k (als. fechado)

$X = V(yz - x^2) \subseteq \mathbb{P}^2$

FUNÇÕES: $f : X \to \mathbb{C}$ localmente um quociente $\frac{p}{q}$ com $p, q : X \to \mathbb{C}$ holomorfas

$f : X \to k$ localmente um quociente $\frac{p}{q}$ com p, q polinómios homogéneos de mesmo grau

---

CORPO DE FUNÇÕES: $\mathcal{M}(X)$

$k(X)$

PARTE II - Superfícies de Riemann e Curvas Algébricas

DEF: X localmente homeomorfo a um aberto de $\mathbb{C}$ com cartas holomorfas

$X = S^2$

$X \subseteq \mathbb{P}^n$ dado pelo anulamento de polinómios homogéneos / k (alg.-fechado)

$X = V(yz - x^2) \subseteq \mathbb{P}^2$

FUNÇÕES: $f : X \to \mathbb{C}$ localmente um quociente $\frac{p}{q}$ com $p, q : X \to \mathbb{C}$ holomorfas

$f : X \to k$ localmente um quociente $\frac{p}{q}$ com p, q polinómios homogéneos de mesmo grau

CORPO DE FUNÇÕES: $\mathcal{M}(X)$

$k(X)$

PARTE II - Superfícies de Riemann e Curvas Algébricas

DEF:	X localmente homeomorfo a um aberto de $\mathbb{C}$ com cartas holomorfas $X = S^2$  	$X \subseteq \mathbb{P}^n$ dado pelo anulamento de polinómios homogéneos / k (alg.-fechado) $X = V(yz - x^2) \subseteq \mathbb{P}^2$
FUNÇÕES:	$f : X \to \mathbb{C}$ localmente um quociente $\frac{p}{q}$ com $p, q : X \to \mathbb{C}$ holomorfas	$f : X \to k$ localmente um quociente $\frac{p}{q}$ com p, q polinómios homogéneos de mesmo grau
CORPO DE FUNÇÕES:	$\mathcal{M}(X)$	$k(X)$

restrições:	X compacto	$\dim X = 1$ e não-singular / liso
MORFISMOS:	$\phi : X \longrightarrow Y$ localmente holomorfo pelas cartas de X e Y.	$\phi : X \subseteq \mathbb{P}^n \longrightarrow Y \subseteq \mathbb{P}^m$ dado por $\phi = (p_0 : \dots : p_m)$ c/ $p_0, \dots, p_m$ homog. de mesmo grau com ϕ bem-definido.
ORDEM DE ANULAMENTO:	para $f \in M(X)^*$ e $p \in X$ $v_p(f)$ = ordem do zero ou polo de f em p	para $f \in k(X)^*$ e $p \in X$ existe uma valorização discreta $v_p : k(X)^* \longrightarrow \mathbb{Z}$

restrições:	X compacto	$\dim X = 1$ e não-singular / liso
MORFISMOS:	$\phi : X \longrightarrow Y$ localmente holomorfo pelas cartas de X e Y.	$\phi : X \subseteq \mathbb{P}^n \longrightarrow Y \subseteq \mathbb{P}^m$ dado por $\phi = (p_0 : \dots : p_m)$ c/ $p_0, \dots, p_m$ homog. de mesmo grau com ϕ bem-definido.
ORDEM DE ANULAMENTO:	para $f \in M(X)^*$ e $p \in X$ $v_p(f)$ = ordem do zero ou polo de f em p	para $f \in k(X)^*$ e $p \in X$ existe uma valorização discreta $v_p : k(X)^* \longrightarrow \mathbb{Z}$

restrições:	X compacto	$\dim X = 1$ e não-singular / liso
MORFISMOS:	$\phi : X \longrightarrow Y$ localmente holomorfo pelas cartas de X e Y.	$\phi : X \subseteq \mathbb{P}^n \longrightarrow Y \subseteq \mathbb{P}^m$ dado por $\phi = (p_0 : \dots : p_m)$ c/ $p_0, \dots, p_m$ homog. de mesmo grau com ϕ bem-definido.
ORDEM DE ANULAMENTO:	para $f \in M(X)^*$ e $p \in X$ $v_p(f)$ = ordem do zero ou polo de f em p	para $f \in k(X)^*$ e $p \in X$ existe uma valorização discreta $v_p : k(X)^* \longrightarrow \mathbb{Z}$

DIVISORES: Nos dois objetos, temos

$$\mathrm{Div}(X) = \left\{ \sum_{p \in X} n_p \cdot P \text{ soma finita} \;\middle|\; n_p \in \mathbb{Z} \right\}$$

Para $f \in M(X)$ (ou $k(X)$) não-nulo, definimos

$$\mathrm{div}(f) = \sum_{p \in X} v_p(f) \cdot p \in \mathrm{Div}(X).$$

Para $D \in \mathrm{Div}(X)$, definimos o espaço vetorial

$$\mathcal{L}(D) = \{0\} \cup \left\{ f \in M(X)^* \text{ (ou } k(X)^*) \;\middle|\; \mathrm{div}(f) \geq -D \right\}$$

Dois importantes teoremas que os dois objetos satisfazem são:

Teorema de Riemann-Roch

Para $D \in \mathrm{Div}(X)$, vale a fórmula

$$\ell(D) - \ell(K_X - D) = 1 - g_X + \deg D$$

($\ell(D) = \dim_{\mathbb{C}\,(\text{ou } k)} \mathcal{L}(D)$)

- K_X: divisor canônico
- g_X: gênero de X

Teorema de Riemann-Hurwitz

Se $f: X \to Y$ é n-cte, temos

$$\chi_X = \deg f \cdot \chi_Y - b$$

(b: ramificação total de f)

onde $\chi = 2 - 2g$ é a característica de Euler.

Dois importantes teoremas que os dois objetos satisfazem são:

Teorema de Riemann-Roch

Para $D \in \mathrm{Div}(X)$, vale a fórmula

$$\ell(D) - \ell(K_X - D) = 1 - g_X + \deg D$$

K_X: divisor canônico; g_X: gênero de X

Teorema de Riemann-Hurwitz ($\mathrm{char}\, k = 0$)

Se $f: X \to Y$ é n-cte, temos

$$\chi_X = \deg f \cdot \chi_Y - b$$

b: ramificação total de f

onde $\chi = 2 - 2g$ é a característica de Euler.

PARTE III - Curvas Elípticas

DEF: (X, O_X) - superfície de Riemann compacta de gênero um

Exemplo: $E_\Lambda := (\mathbb{C}/\Lambda, 0+\Lambda)$ onde $\Lambda \subseteq \mathbb{C}$ é um reticulado.

De fato, toda curva elíptica (X, O_X) admite um isomorfismo

$$(X, O_X) \xrightarrow{\simeq} (\mathbb{C}/\Lambda, 0+\Lambda)$$

PARTE III - Curvas Elípticas

DEF: (X, O_X) - superfície de Riemann compacta de gênero um

Exemplo: $E_\Lambda := (\mathbb{C}/\Lambda, 0+\Lambda)$ onde $\Lambda \subset \mathbb{C}$ é um reticulado.

De fato, toda curva elíptica (X, O_X) admite um isomorfismo

$$(X, O_X) \xrightarrow{\simeq} (\mathbb{C}/\Lambda, 0+\Lambda)$$

Em $\mathcal{M}(E_\Lambda)$, existe uma função especial chamada função $\wp$ de Weierstrass:

$$\boxed{\wp_\Lambda = \wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)}$$

$$\Rightarrow \wp'(z;\Lambda) = \sum_{\lambda \in \Lambda \setminus \{0\}} -\frac{2}{(z-\lambda)^3}$$

Algumas propriedades de $\wp_\Lambda$ são

- $\wp_\Lambda$ é par $\left(\wp_\Lambda(z;\Lambda) = \wp_\Lambda(-z;\Lambda) \right)$
- $0+\Lambda$ é o único polo de $\wp_\Lambda$, de ordem 2 $\left(v(\wp) = -2 \right)$

Algumas propriedades de $\wp_\Lambda$ são

- $\wp_\Lambda$ é par $\left(\wp_\Lambda(z;\Lambda) = \wp_\Lambda(-z;\Lambda) \right)$
- $0+\Lambda$ é o único polo de $\wp_\Lambda$, de ordem 2 $\left(v(\wp) = -2 \right)$

★ $\wp_\Lambda$ e $\wp_\Lambda'$ satisfazem uma relação algébrica em $\mathcal{M}(E_\Lambda)$:

$$\left(\wp_\Lambda'\right)^2 = 4\wp_\Lambda^3 - 60\, G_4(\Lambda)\wp_\Lambda - 140\, G_6(\Lambda)$$

onde $G_{2k}(\Lambda) := \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^{2k}}$, $k \geq 2$.

Para todo $\Lambda \subseteq \mathbb{C}$ reticulado, o polinômio

$$4x^3 - 60\,G_2(\Lambda)x - 140\,G_6(\Lambda)$$

possui três raízes distintas.

Para todo $\Lambda \subseteq \mathbb{C}$ reticulado, o polinômio

$$4x^3 - 60 G_2(\Lambda) x - 140 G_6(\Lambda)$$

possui três raízes distintas. Assim

$$E_\Lambda : y^2 z = 4x^3 - 60 G_2(\Lambda) x z^2 - 140 G_6(\Lambda) z^3 \subseteq \mathbb{P}^2$$

é uma superfície de Riemann e também uma curva algébrica lisa / $\mathbb{C}$.

Para todo $\Lambda \subseteq \mathbb{C}$ reticulado, o polinômio

$$4x^3 - 60 G_2(\Lambda) x - 140 G_6(\Lambda)$$

possui três raízes distintas. Assim

$$E_\Lambda : y^2 z = 4x^3 - 60 G_2(\Lambda) x z^2 - 140 G_6(\Lambda) z^3 \subseteq \mathbb{P}^2$$

é uma superfície de Riemann e também uma curva algébrica lisa / $\mathbb{C}$.

E mais, o mapa

$$\begin{aligned} (E_\Lambda, O_X) &\longrightarrow (\mathcal{E}_\Lambda, O) \\ z + \Lambda &\longmapsto \begin{cases} (\wp(z) : \wp'(z) : 1) & z \notin \Lambda \\ O = (0:1:0) & z \in \Lambda \end{cases} \end{aligned}$$

é um isomorfismo.

isogenia: $f : E_\Lambda \longrightarrow E_{\Lambda'}$ holomorfa e não-constante

tal que $f(0+\Lambda) = 0+\Lambda'$.

Daí, definimos

$$\mathrm{Hom}(E_\Lambda, E_{\Lambda'}) := \{0\} \cup \{f : E_\Lambda \longrightarrow E_{\Lambda'} \mid f \text{ isogenia}\}$$

$$\mathrm{End}(E_\Lambda) := \mathrm{Hom}(E_\Lambda, E_\Lambda)$$

isogenia: $f : E_\Lambda \longrightarrow E_{\Lambda'}$ holomorfa e não-constante

tal que $f(0+\Lambda) = 0+\Lambda'$.

Daí, definimos

$$\mathrm{Hom}(E_\Lambda, E_{\Lambda'}) := \{0\} \cup \{f : E_\Lambda \longrightarrow E_{\Lambda'} \mid f \text{ isogenia}\}$$

$$\mathrm{End}(E_\Lambda) := \mathrm{Hom}(E_\Lambda, E_\Lambda)$$

☆ Pode-se mostrar que todo $f \in \mathrm{Hom}(E_\Lambda, E_{\Lambda'})$ é da forma

$$f_\alpha : z + \Lambda \longmapsto \alpha z + \Lambda' \qquad \alpha \in \mathbb{C} \text{ com } \alpha\Lambda \subseteq \Lambda'$$

Assim, temos as identificações:

$$\mathrm{Hom}(E_\Lambda, E_{\Lambda'}) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda'\} \text{ e } \mathrm{End}(E_\Lambda) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$$

Para todo $\Lambda \subseteq \mathbb{C}$ reticulado, $\mathrm{End}(E)$ contém os mapas

$$[n]: \begin{array}{ccc} E_\Lambda & \longrightarrow & E_\Lambda \\ z + \Lambda & \longmapsto & nz + \Lambda \end{array} \qquad n \in \mathbb{Z}$$

o que nos dá um mapa

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathrm{End}(E_\Lambda). \\ n & \longmapsto & [n] \end{array}$$

Se tal mapa <u>não</u> for sobrejetor, dizemos que E_Λ (ou Λ) admite <u>multiplicação complexa</u> (por $R = \mathrm{End}(\Lambda) \subseteq \mathbb{C}$).

Para todo $\Lambda \subseteq \mathbb{C}$ reticulado, $\mathrm{End}(E)$ contém os mapas

$$[n]: \begin{array}{ccc} E_\Lambda & \longrightarrow & E_\Lambda \\ z + \Lambda & \longmapsto & nz + \Lambda \end{array} \qquad n \in \mathbb{Z}$$

o que nos dá um mapa $\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathrm{End}(E_\Lambda). \\ n & \longmapsto & [n] \end{array}$

Se tal mapa <u>não</u> for sobrejetor, dizemos que E_Λ (ou Λ) admite <u>multiplicação complexa</u> (por $R = \mathrm{End}(\Lambda) \subsetneq \mathbb{C}$).

<u>Exemplos</u>: $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ com $\mathbb{Q}(\tau)/\mathbb{Q}$ de grau dois. $(\tau \notin \mathbb{R})$

Em particular, os anéis de inteiros algébricos $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$ com $\omega = e^{2\pi i/3}$.

Para $n \geq 2$, $[n] : E_\Lambda \longrightarrow E_\Lambda$ é um homomorfismo de grupos abelianos cujo núcleo $E_\Lambda[n]$ são chamados pontos de n-torção.

se $\Lambda = \mathbb{Z}\lambda_1 + \mathbb{Z}\lambda_2$, então

$$E_\Lambda[n] = \left\{ \left(r \cdot \frac{\lambda_1}{n} + s \cdot \frac{\lambda_2}{n} \right) + \Lambda \;\middle|\; 0 \leq r, s < n \right\}$$

o que implica que $E_\Lambda[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$.

DEF: (X, O_X) - curva algébrica projetiva e lisa de gênero um.

Neste caso, existem $x, y \in k(X)$ chamadas coordenadas de Weierstrass tais que

$$\begin{aligned} \phi : (X, O_X) &\longrightarrow \mathbb{P}^2 \\ P &\longmapsto (x(P) : y(P) : 1) \\ &\quad \ulcorner (0:1:0) \end{aligned}$$

induz um isomorfismo de (X, O_X) com $(E, 0)$ cúbica de Weierstrass lisa

DEF: (X, O_X) - curva algébrica projetiva e lisa de gênero um.

Neste caso, existem $x, y \in k(X)$ chamadas coordenadas de Weierstrass tais que

$$\begin{aligned} \phi : (X, O_X) &\longrightarrow \mathbb{P}^2 \\ P &\longmapsto (x(P) : y(P) : 1) \end{aligned}$$

$\ulcorner (0:1:0)$

induz um isomorfismo de (X, O_X) com $(E, 0)$ cúbica de Weierstrass lisa, ou seja, $E \subseteq \mathbb{P}^2$ dada por

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

para certos $a_1, a_2, a_3, a_4, a_6 \in k$.

Se $\text{char } k \neq 2, 3$ toda curva elíptica será isomorfa a uma cúbica de Weierstrass lisa dada por

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

onde Δ e j são dados por

$$\Delta = -16(4A^3 + 27B^2) \qquad j = -1728\frac{(4A)^3}{\Delta}$$

Algumas propriedades são:

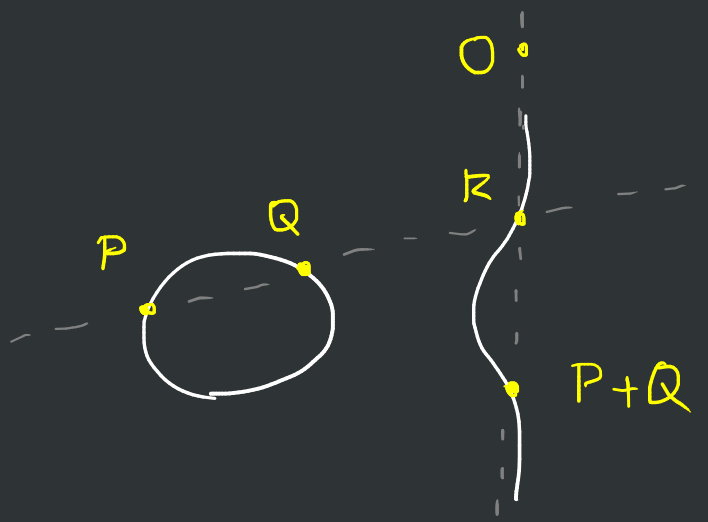
- $\Delta \neq 0$ pois E é lisa
- j parametriza as classes de k-isomorfismo de curvas elípticas

Sobre os pontos de (X, O_X) podemos definir uma operação de grupo

Para $(X, O_X) = (E, O) \subseteq \mathbb{P}^2$ cúbica de Weierstrass lisa definimos

$$P + Q$$

de modo que O é o elemento neutro e "pontos colineares somam zero":



isogenia: $\phi : (E, O_E) \longrightarrow (E', O_E)$ mapa não-constante

Novamente, toda isogenia é um homomorfismo de grupos.

Exemplo: $[n] : E \longrightarrow E$ multiplicação por n, $n \in \mathbb{Z}$

Para $n \geq 2$, o núcleo $E[n]$ são os pontos de n-torção

Se $\operatorname{char} k = 0$, temos $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Definimos

$$\mathrm{Hom}(E, E') = \{0_{E'}\} \cup \{\phi : E \longrightarrow E' \text{ isogenia}\}$$

$$\mathrm{End}(E) = \mathrm{Hom}(E, E')$$

$$\mathrm{Aut}(E) = \mathrm{End}(E)^*$$

Temos as seguintes propriedades:

- $\mathrm{End}(E) = \begin{cases} \mathbb{Z} \\ \mathbb{Z} \text{ ordem em um corpo quadrático imaginário} \\ \mathbb{Z} \text{ ordem em uma álgebra de quatérnions} \end{cases}$ } $\mathrm{char}\, k = 0$
- $\mathrm{Aut}(E)$ é finito

PARTE IV - Teoria Algébrica dos Números - CFT Global

K - corpo de números algébricos

L - extensão finita e abeliana de K com $n = [L:K]$

Já sabemos que para $K = \mathbb{Q}$, os corpos ciclotômicos satisfazem o

Teorema de Kronecker - Weber

Se $L/\mathbb{Q}$ é finita e abeliana, então $L \subseteq \mathbb{Q}(\zeta_n)$ para algum $n \geq 1$

No caso geral, temos a seguinte generalização de $\mathbb{Q}(\zeta_n)$

$K(\mathfrak{a})$: ray class field módulo $\mathfrak{a}$, onde $\mathfrak{a} \triangleleft \mathcal{O}_K$ é não-nulo.

No caso geral, temos a seguinte generalização de $\mathbb{Q}(\zeta_n)$

$K(\mathfrak{a})$: ray class field módulo $\mathfrak{a}$, onde $\mathfrak{a} \triangleleft \mathcal{O}_K$ é não-nulo.

E estas extensões satisfazem

(K-W) $K(\mathfrak{a})/K$ é finita e abeliana e toda extensão finita e abeliana de K está contida em $K(\mathfrak{a})$ para algum $\mathfrak{a}$.

Para $\mathfrak{a} = \mathcal{O}_K$, obtemos $H = K(\mathcal{O}_K)$, também chamado de corpo de classe de Hilbert de K.

PARTE V - Multiplicação Complexa

Seja $K/\mathbb{Q}$ um corpo quadrático imaginário. Consideramos

$$Ell(\mathcal{O}_K) = \frac{\{\text{curvas elípticas } E/\mathbb{C} \text{ com } End(E) \cong \mathcal{O}_K\}}{\mathbb{C}\text{- isomorfismo}}$$

Exemplo: $E_\Lambda : y^2z = 4x^3 - 60G_2(\Lambda)xz^2 - 140G_6(\Lambda)z^3 \in Ell(\mathcal{O}_K)$

para $\Lambda = \mathcal{O}_K \simeq \mathbb{Z} + \mathbb{Z}\tau$

Obs.: Pode-se mostrar que $Ell(\mathcal{O}_K)$ é finito com $h_K = \#\, cl(\mathcal{O}_K)$ elementos.

Se $E \in Ell(\mathcal{O}_K)$, temos

- O j-invariante $j(E)$ é um inteiro algébrico com $K(j(E)) = H$.
- e $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K$

Em particular, para K com $h_K = 1$, $j(E) \in \mathbb{Z}$.

Aplicação:

A função

$(\operatorname{Im}\tau > 0) \qquad \tau \longrightarrow j(\tau) := j(\mathcal{E}_\Lambda)$ com $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$

$$\mathcal{E}_\Lambda : y^2 z = 4x^3 - 60 G_2(\Lambda) x z^2 - 140 G_6(\Lambda) z^3$$

será uma função analítica complexa, que pode ser expandida como

$$j(\tau) = \frac{1}{q} + 744 + 196884 q + O(q^2), \qquad q = e^{2\pi i \tau}$$

Para $\tau = \dfrac{1+\sqrt{-163}}{2}$, $\quad q = e^{2\pi i \tau} = -\dfrac{1}{e^{\pi\sqrt{163}}}$

Agora, usando o fato de que $h_K = 1$ para $K = \mathbb{Q}\left(\frac{1+\sqrt{-163}}{2}\right)$:

$$\underbrace{j\left(\frac{1+\sqrt{-163}}{2}\right)}_{\in \mathbb{Z}} = -e^{\pi\sqrt{163}} + 744 + 196884q + O(q^2)$$

$$\Rightarrow \quad e^{\pi\sqrt{163}} = \underbrace{-j\left(\frac{1+\sqrt{-163}}{2}\right) + 744}_{\in \mathbb{Z}} + \varepsilon$$

Agora, usando o fato de que $h_K = 1$ para $K = \mathbb{Q}\left(\frac{1+\sqrt{-163}}{2}\right)$:

$$\underbrace{j\left(\frac{1+\sqrt{-163}}{2}\right)}_{\in \mathbb{Z}} = -e^{\pi\sqrt{163}} + 744 + 196884q + O(q^2)$$

$$\Rightarrow \quad e^{\pi\sqrt{163}} = \underbrace{-j\left(\frac{1+\sqrt{-163}}{2}\right) + 744}_{\in \mathbb{Z}} + \varepsilon$$

De fato, $e^{\pi\sqrt{163}} = n + 0.\underbrace{999\ldots9}_{12}250072\ldots$

Para $E \in Ell(\mathcal{O}_K)$, temos um isomorfismo "normalizado"

$$[\cdot] : \mathcal{O}_K \longrightarrow End(E)$$

Para $E \in Ell(\mathcal{O}_K)$, temos um isomorfismo "normalizado"

$$[\cdot] : \mathcal{O}_K \longrightarrow End(E)$$

Assim, definimos para $a \triangleleft \mathcal{O}_K$ não-nulo o conjunto dos pontos de a-torção.

$$E[a] := \{ P \in E : [\alpha](P) = 0 \quad \forall \alpha \in a \}$$

Para $a = m\mathcal{O}_K$. $m \in \mathbb{Z}$, recuperamos $E[a] = E[m]$.

Para todo $m \geq 2$,

$$L_m := K(j(E), E[m])$$

coordenadas

é uma extensão abeliana de $K(j(E))$ e não-necessariamente de K.

Para todo $m \geq 2$,

$$L_m = K(j(E), E[m])$$

coordenadas

é uma extensão abeliana de $K(j(E))$ e não-necessariamente de K.

Daí, para obter extensões abelianas de K, usamos um mapa adequado $h : E \longrightarrow \mathbb{P}^1$ chamada função de Weber.

Para todo $m \geq 2$,

$$L_m = K(j(E), E[m])$$

coordenadas

é uma extensão abeliana de $K(j(E))$ e não-necessariamente de K.

Daí, para obter extensões abelianas de K, usamos um mapa adequado $h : E \longrightarrow \mathbb{P}^1$ chamada função de Weber.

Exemplo: Se $E \subseteq \mathbb{P}^2$ é dada por

$$Y^2Z = X^3 + AXZ^2 + BZ^3 \qquad A, B \in H$$

um exemplo é $h(x,y) = h(x:y:1) = \begin{cases} x & \text{se } AB \neq 0 \\ x^2 & \text{se } B = 0 \\ x^3 & \text{se } A = 0 \end{cases}$

Por fim, temos o seguinte:

Por fim, temos o seguinte:

Se $E/H \in Ell(\mathcal{O}_K)$ com função de Weber $h : E \longrightarrow \mathbb{P}^1$, então para todo $\mathfrak{a} \lhd \mathcal{O}_K$ não-nulo

$$K(j(E), h(E[\mathfrak{a}]))$$

é o ray class field módulo $\mathfrak{a}$.

Por fim, temos o seguinte:

Se $E/H \in Ell(\mathcal{O}_K)$ com função de Weber $h : E \longrightarrow \mathbb{P}^1$, então para todo $\mathfrak{a} \triangleleft \mathcal{O}_K$ não-nulo

$$K(j(E), h(E[\mathfrak{a}]))$$

é o ray class field módulo $\mathfrak{a}$.

Exemplo: $E : Y^2Z = X^3 + XZ^2 \in Ell(\mathcal{O}_K)$ para $K = \mathbb{Q}(i)$

Temos para $\mathfrak{a} \triangleleft \mathcal{O}_K$ não-nulo:

$$\mathbb{Q}(i)[\mathfrak{a}] = \mathbb{Q}(i)\left(\{x^2 \mid (x:y:1) \in E[\mathfrak{a}]\}\right)$$

FIM

Muito obrigado pela atenção !!!

:)