

4. Waluacje dyskretne

Kryterium nieosobliwości krzywej afinicznej $C \in K[X, Y]$

Twierdzenie

Krzywa zadana równaniem Weierstrassa jest osobliwa wtedy i tylko wtedy gdy $\Delta = 0$

Dowód

Izomorfizm φ (dopuszczalna zmiana zmiennych zachwuje niezerowość wyróżnika Δ), więc wystarczy rozważać postać normalną krzywej.

Założmy, że $\text{char}(K) \neq 2$ i $\text{char}(K) \neq 3$, wtedy:

$$E: Y^2 = X^3 + a_4X + a_6, \quad \Delta = -16(4a_4^3 + 27a_6^2)$$

Z drugiej strony na mocy wzorów CARDANO mamy, że wielomian

$X^3 + a_4X + a_6$ ma pierwiastki wielokrotne wtedy i tylko wtedy, gdy :

$$\left(\frac{a_6}{2}\right)^2 + \left(\frac{a_4}{3}\right)^3 = 0 \quad \text{tj. gdy } \Delta = 0$$

Zatem istnieje równanie układu

$$\frac{\delta E}{\delta Y} = 2Y = 0$$

$$\frac{\delta E}{\delta X} = \frac{\delta}{\delta X}(x - x_1)^2(x - x_2)(-1) = -[2(x - x_1)(x - x_2) + (x - x_1)^2]$$

Zatem punkt $(x_1, 0)$ jest punktem osobliwym krzywej E. Odwrotnie jeśli punkt p jest punktem osobliwym krzywej E to $\Delta = 0$.

Niech:

R- dowolny (przemienny z 1)

R* - oznacza grupą jedności pierścienia R

Definicja

Waluację dyskretną pierścienia R nazywamy funkcję addytywną

$v: R \rightarrow (0, \infty]$ spełniającą następujący warunek „trójkąta” tzn.

$$\forall a, b \in R \quad v(a+b) \geq \min(v(a), v(b))$$

Wniosek

Waluacja v spełnia następujące warunki:

a) $v(0) = \infty$

b) $a \in R^* \rightarrow v(a) = 0$

Dowód

1) Z addytywności:

Gdyby $v(0) < \infty$ to $v(0) = v(0 \cdot a) = v(a) \cdot v(0) \Rightarrow 0 = v(a)$ dla dowolnego $a \in R$, co jest niemożliwe. Zatem $v(0) = \infty$ c.b.d.o

2) Mamy $v(a) = 0(a \cdot 1) = v(a) + v(1) \Rightarrow v(1) = 0$. Dalej jeżeli $a \in R$ oraz istnieje

$b \in R$ takie, że $ab = 1$, to wtedy

$$0 = v(1) = v(a \cdot b) = v(a) + v(b) \Rightarrow v(a) = v(b) = 0 \text{ c.b.d.o}$$

Definicja

Jeżeli w pierścieniu istnieje element nieodwracalny $n \in R \setminus \{R^* \cup \{0\}\}$ taki że dowolny $s \in R \setminus \{0\}$ można przedstawić w postaci $s = n^d t$, $d \in \mathbb{N}_0$, $t \in R^*$, to n nazywamy parametrem lokalnym.

Wniosek

Wartość d jest określona jednoznacznie.

Dowód

$s = n^{d_1} \cdot t_1 = n^{d_2} \cdot t_2$ wtedy $1 = n^{d_1 d_2} t_1 t_2^{-1} \Rightarrow n^{d_1 d_2} = t_2 t_1^{-1}$ co jest niemożliwe, gdyż lewa strona równania jest elementem nieodwracalnym w R a prawa strona równania jest elementem odwracalnym. Otrzymana sprzeczność dowodzi że $d_1 = d_2$.

Uwaga

W pierścieniu lokalnym $\mathcal{O}_p(E)$ dowolna prosta afiniczna, która nie jest „styczna” do krzywej E w punkcie P jest parametrem lokalnym.

Definicja

Punkt $P \in E, P=(x, y)$ jest punktem rzędu 2 wtedy i tylko wtedy, gdy $P=\bar{P}$ (sprzężone) tj. $y = \bar{y} = -y - a_1x - a_3$.

Twierdzenie

Każdy element $r \in O_P$ można przedstawić w postaci $s = n^d \cdot t, d \in N_0, t \in R^*,$ gdzie $n \in m_P(E)$.

Gdzie:

$m_P(E)$ - ideał maksymalny pierścienia lokalnego $O_P(E)$

Jeśli $f(P) \neq 0$ to f jest jednością pierścienia i (1) zachodzi dla $d=0$.

Założmy więc, że f nie jest jednością tj. $f(P) = 0$

Pokażemy, że $u = X - x$ jest parametrem lokalnym w pierś $O_P(E)$ cieniu

Każdy $f \in K[E]$ można przedstawić w postaci:

$$\begin{aligned} 0 \neq f &= u(x) + Y \cdot W(x) \\ f &\in K[X, Y] \end{aligned}$$

Niech $f = (X - x)^{d_1} (X_1 + Y_{w_1}) = (X - x)^{d_1} f_g$

gdzie $(X - x)^{d_1}$ jest maksymalną potęgą dzielącą zarówno $u(x)$ jak i $w(x)$. Ponieważ $f \neq 0$, więc v_1 lub $w_1 \neq 0$.

Jeśli $f_1(P) \neq 0$ to f_1 – jedność to (1) zachodzi dla $d = d_1$

Jeśli $\bar{f}_1(P) \neq 0$ to $\bar{f}_1$ – jedność oraz mamy:

$$f_1 = N(f_1)(\bar{f}_1)^{-1}$$

gdzie $N(f_1) \in K[X]$

Zatem niech

$$N(f_1) = (X - x)^{d_2} f_2$$

gdzie f_2 – jedność, wtedy (1) zachodzi dla $d = d_1 + d_2$

Pozostały przypadek to $f_1(P) = \bar{f}_1(P) = 0$ (*)

Pokażemy, że tak się nie może zdarzyć, w tym celu rozważmy układ równań postaci:

$$\begin{pmatrix} 1 & Y(P) \\ 1 & \bar{Y}(P) \end{pmatrix} \begin{pmatrix} v_1 \\ w_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

który ma rozwiązanie niezerowe (v_1, w_1) na mocy (*)

Ale wyznacznik macierzy wynosi $\bar{Y}(P) - Y(P) \neq 0$ (gdyż P nie jest punktem rzędu 2) co przeczy założeniu, że powyższy układ ma rozwiązanie niezerowe i tym samym kończy dowód twierdzenia.

Wniosek

Dla dowolnego $P \in E$ i $f \in K[E]$ wartość $d = d(f)$ o której mowa w twierdzeniu, nazywamy rzędem funkcji f w punkcie P . Onznaczamy $\text{ord}_P f$. Pojęcie rzędu rozszerzamy na dowolną funkcję wymierną $r = \frac{f}{g}$

jak poniżej:

$$\text{ord}_P 0 = \infty$$

$$\text{ord}_P \frac{f}{g} = \text{ord}_P f - \text{ord}_P g$$

W dalszym ciągu będziemy rozważać rozszerzenie pojęcia waluacji dyskretnej $v: R \rightarrow (-\infty, +\infty]$ spełniające warunek addytywności i trójkąta.

Stwierdzenie

Dla dowolnego $P \in E$ $\text{ord}_P: K(E) \rightarrow \mathbb{Z} \cup \{\infty\}$ jest waluacją dyskretną.

Dowód

Warunek addytywności jest rzeczywisty.

Założmy teraz, że:

$$s = \frac{f_1}{f_2} = \frac{u^{d_1} t_1}{u^{d_2} t_2}$$

$$s' = \frac{f'_1}{f'_2} = \frac{u^{d'_1} t'_1}{u^{d'_2} t'_2}$$

Wtedy:

$$s + s' = u^{d_1 - d_2} (t_1 t_2^{-1}) + u^{d'_1 - d'_2} (t'_1 (t'_2)^{-1}) = u^\delta (t u^{d_1 - d_2 - \delta} + t')$$

$$\text{gdzie } \delta = \min(d_1 - d_2, d'_1 - d'_2) \text{ i } d_1 - d_2 \geq d'_1 - d'_2, \quad t \text{ i } t'$$

są jednościami.

Zatem $\text{ord}_P(s + s') \geq \delta = \min(\text{ord}_P s, \text{ord}_P s')$ C.N.D.

5. Krzywe eliptyczne rzutowe

5.1 Płaszczyzna rzutowa

Niech K -ciało algebraiczne domknięte

W zbiorze $K^3 \setminus \{0\}$ określającą relację równoważności, zadaje jak następuje

$(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ wtt.

$\text{exist } \lambda \in K^* (x_2, y_2, z_2) = (\lambda x_1, \lambda y_1, \lambda z_1)$

Zbiór klas abstrakcji: $K^3 \setminus \{0\}$ nazywamy płaszczyznę rzutową i oznaczamy $P^2(K)$

Przykład

Przestrzeń rzutowa $P^1(K)$ można identyfikować dowolnym punktem na prostej $y=1$ lub prostej $y=0$

W zbiorze $P^2(K)$ możemy wyodrębnić podzbiór "punktów skończonych" płaszczyzny rzutowej odpowiadająca cyklicznym kierunkom równoległych do płaszczyzny $z=0$

Odwrotnie jeśli $Q = (x, y, z) \in P^2(K)$ to jego "odjednorodnienie" definiujemy.

W ten sposób każdemu punktowi afinicznemu można przyporządkować jego ujednorodnienie $Q^* \in P^2(K)$ a każdemu punktowi $Q \in P^2(K)$ jego odjednorodnienie $Q_* \in A^2(K)$.

Operację $(*)$ nazywamy ujednorodnieniem i odjednorodnieniem odpowiednio.

Niech :

$$\phi: A^2(K) \rightarrow P^2(K)$$

$$Q \rightarrow Q^*$$

$$\psi: P^2(K) \rightarrow A^2(K)$$

$$Q \rightarrow Q_*$$

Wtedy mamy:

$$\psi \circ \phi = Id_{A^2(K)}$$

$$\phi \circ \psi = Id_U$$

Gdzie $U \in P^2(K)$ jest zbiorem punktów skończonych płaszczyzny rzutowej $P^2(K)$ (ze względu na ustaloną współrzędną)

Ujednorodnienie i odjednorodnienie wielomianów

Operacje "*" p rzutuje się w sposób naturalny na wielomiany

$$f \in K[X, Y]$$

$$\phi: K[X, Y] \rightarrow K[X, Y, Z]_{hom}$$

$$\phi: f \rightarrow F$$

$$F(X, Y, Z) = f\left(\frac{X}{Z}, \frac{Y}{Z}\right) * Z^{st f}$$

gdzie $K[X, Y, Z]_{hom}$ jest zbiorem wielomianów jednorodnych tzn spełniających warunek $F(\lambda X, \lambda Y, \lambda Z) = \lambda^{st F} F(X, Y, Z)$

Podobnie definiujemy :

$$\psi: K[X, Y, Z]_{hom} \rightarrow K[X, Y]$$

$$F \rightarrow f$$

$$f(X, Y) = F(X, Y, Z)$$

mamy równość:

$$\phi \circ \psi = Id$$

$$\psi \circ \phi = Id$$

na odpowiednich dziedzinach zachodzi następująco:

Lemat

Mamy dla $f \in K[X, Y]$, $F \in K[X, Y, Z]_{hom}$

$$1) (fg)^* = f^* g^*$$

$$2) (FG)^* = F^* G^*$$

$$3) (f^*)^* = f$$

$$4) \text{ Jeśli } Z^* F \text{ to } (F_*)^* = F$$

5.2 Krzywe rzutowe

Niech C -krzywa algebraiczna płaska. Zatem $C[X, Y]$ jest wielomianem nieoznakowanym $K[X, Y]$.

Krzywe rzutowe C^* definiujemy jako krzywe zadane przez ujednorodnienie $C^*[X, Y, Z]$ wielomianami $C[X, Y]$. Zauważmy, że $C^*[X, Y, Z]$ jest rozkładem wtedy i tylko wtedy gdy $C[X, Y]$

Pierścień ilorazowy

$K[X, Y, Z]/C^*$ nazywamy pierścieniem współrzędnych dla krzywej rzutowanej C^* oznaczamy go $K[C^*]$.

Aby funkcja wymierna $r = \frac{F}{G}$ była dobrze określona na $P^2(K)$ F i G muszą być wielomianami tego samego stopnia $\text{st}(F) = \text{st}(G)$.

Zatem $K(C^*) = \{r = \frac{F}{G}; G, F \in K[X, Y, Z] \text{ hom}/C^*, \text{st } F = \text{st } G\}$.

Lokalizując $K(C^*)$ w punkcie $P^* \in C^*$ otrzymujemy pierścień lokalny

$O_{P^*}(C^*)$, dokładniej $O_{P^*}(C^*) = \{r = \frac{F}{G} \in K(C^*); G(P) \neq 0\}$.

Analogicznie mamy $\phi: K(C^*) \rightarrow K(C)$ $\frac{F}{G} \rightarrow \frac{F^*}{G^*} = \frac{F(X, Y, Z)}{G(X, Y, Z)}$

aby $\phi(r)$ było dobrze zdefiniowane położymy

$$\phi(r) = \phi\left(\frac{F}{G}\right) = \frac{Z^{\text{st } F} F\left(\frac{X}{Z}, \frac{Y}{Z}\right)}{Z^{\text{st } G} G\left(\frac{X}{Z}, \frac{Y}{Z}\right)} = \frac{F\left(\frac{X}{Z}, \frac{Y}{Z}\right)}{G\left(\frac{X}{Z}, \frac{Y}{Z}\right)}, \text{ wtedy}$$

$$\phi(r)(\lambda x, \lambda y, \lambda z) = \frac{F\left(\frac{\lambda X}{\lambda Z}, \frac{\lambda Y}{\lambda Z}\right)}{G\left(\frac{\lambda X}{\lambda Z}, \frac{\lambda Y}{\lambda Z}\right)} = \frac{F\left(\frac{X}{Z}, \frac{Y}{Z}\right)}{G\left(\frac{X}{Z}, \frac{Y}{Z}\right)} = \phi(r)(X, Y, Z) \quad \text{więc}$$

$\phi(r)$ nie zależy od reprezentanta klasy abstrakcji relacji “r”

Wiosek

Mamy równość:

$$\psi \circ \phi = \text{Id}_{K(C)}$$

$$\phi \circ \psi = \text{Id}_{K(C^*)}$$

Dowód

$$\psi(\phi(r)(x, y)) \cdot \psi\left(\frac{F(\frac{X}{Z}, \frac{Y}{Z})}{G(\frac{X}{Z}, \frac{Y}{Z})}\right) = r(x, y) \quad \text{więc} \quad \psi(\phi(r)) = r$$

$$\psi(\phi(R)(x, y, z)) = \phi(R(x, y, 1)) = R\left(\frac{x}{y}, \frac{y}{z}, 1\right) = \left(\frac{F(\frac{X}{Z}, \frac{Y}{Z}, 1)}{G(\frac{X}{Z}, \frac{Y}{Z}, 1)}\right) =$$

$$= \frac{Z^{-st} F(X, Y, Z)}{Z^{-st} G(X, Y, Z)} = R(X, Y, Z) \quad \text{więc} \quad \phi \circ \psi(R) = R$$

Uwaga

Ponieważ operacja (*) jest homomorfizmem więc x,y

$$\phi(r, s)(x, y) = \phi\left(\frac{F}{G}, \frac{F'}{G'}\right) = \phi\left(\frac{FF'}{GG'}\right) = \frac{F(\frac{X}{Z}, \frac{Y}{Z})}{G(\frac{X}{Z}, \frac{Y}{Z})} \cdot \frac{F'(\frac{X}{Z}, \frac{Y}{Z})}{G'(\frac{X}{Z}, \frac{Y}{Z})} = \phi(r) \cdot \phi(s)$$

i podobnie

$$\phi(R, S)(X, Y, Z) = \psi\left(\phi\left(\frac{FF'}{GG'}\right)(X, Y, Z)\right) = \frac{F(X, Y, Z) F'(X, Y, Z)}{G(X, Y, Z) G'(X, Y, Z)} = \psi(R) \cdot \psi(S)$$

Definicja

Rzutowanym równaniem weierstrassa nazywamy równanie postaci :

$E^* : X^{2Z} + a_1 XYZ + a_3 XZ^3 = x^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3$ a krzywą E^* zadaną tym równaniem rzutowaniem krzywej afinicznej E (lub domknięciem rzutowym E)

Powiedzmy, że dwie krzywe E, E' zadane odpowiednim równaniem Weierstrassa są izomorficzne wtedy i tylko wtedy gdy istnieje dopuszczalna zamiana zmiennych przeprowadzająca jedną krzywą w drugą

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \rightarrow \begin{pmatrix} u^2 X + r^2 \\ u^3 Y + u^2 sX + 2 \\ z \end{pmatrix} \quad \text{gdzie} \quad u, r, s, t \in K, u \neq 0 \quad \text{z uwzględnieniem dzielenia}$$

obu stron równania przez u^6 . Krzywą rzutową nazywamy nieosobliwą, jeżeli wyróżnik Δ jest różny od 0 co jest zgodne z oryginalną definicją nieosobliwości (przez pochodne cząstkowe)

Definicja

E^* - nazywamy krzywą eliptyczną rzutową wtedy i tylko wtedy gdy jest nieosobliwa to jest gdy $\Delta \neq 0$

Wniosek

Krzywa Eliptyczna rzutowa E^* składa się z punktów skończonych (które uzyskujemy przez odjednorodnienie E^*) oraz punktu w nieskończoności

$$\Theta = (0, 1, 1) \quad .$$

Dowód

Odjednorodniając wielomian opisujący krzywą E^* ze względu na $z \neq 0$ otrzymujemy krzywą eliptyczną E (punkty skończone). Jeśli natomiast

$z=0$ to równanie E^* wynika, że $X=0$, otrzymujemy punkt $(0, Y, 0) = (0, 1, 0)$

Twierdzenie

Niech $P^* \in E^*$ (E^* - krzywa eliptyczna rzutowa), wtedy $\mathcal{O}_{P^*}(E^*)$ jest pierścieniem z waluacją dyskretną.

Dowód

Jeżeli P^* - skończony to było to już udowodnione, jeśli $P^* = \Theta$ to pokażemy, że parametrem lokalnym ze względu na zmienne Y jest $u = \frac{X}{Y}$

Dla dowolnej rozważmy odjednorodnienie E krzywe E^* ze względu na Y .

$E : Z + a_1 XZ + a_3 Z^3 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3$ Wystarczy pokazać, że $u=X$ jest parametrem lokalnym krzywej E w punkcie $(0,0)$ gdyż

$$(0, 1, 0) = \left(\frac{0}{1}, \frac{0}{1} \right)$$

Zauważmy że X jest dzielnikiem Z w pierścieniu $\mathcal{O}_{(0,0)}(E)$, gdyż

$$Z = \frac{Zx^3}{x^3} = \frac{Zx^3}{Z + \dots - a_6 Z^3} = x^3 \frac{1}{1 + a_1 x + \dots + a_6 x^2} \quad (1)$$

zatem

$$x^3 | Z \quad \text{więc} \quad x | Z \quad .$$

Niech teraz $f \in K[E]$ będzie zapisany w postaci

$$f = r(Z) + s(Z)X + t(Z)X^2 \quad .$$

Wyciągniemy najwyższą potęgę Z w każdym wielomianie r, s, t i napiszemy $f = r_1(Z)Z^i + s_1(Z)Z^j X + t_1(Z)Z^k X^2$, gdzie ZXr_1 lub ZXs_1 lub ZXt_1 lub $r_1=0$ lub $s_1=0$ lub $t_1=0$.

Zastępując Z przez postać (1) dostaniemy, że:

$f = r_1\left(\frac{x^3}{1} + \dots\right) + s_1\left(\frac{x^3}{1} + \dots\right)X + t_1\left(\frac{x^3}{1} + \dots\right) = r_2 X^3 + s_2 X^{3j+1} + t_2 X^{3k+2}$ gdzie $r_2, s_2, t_2 \in K(E)$, każdy z nich jest albo regularny w punkcie $(0, 0)$ albo tożsamościowo równy zero w $K(E)$.

Niech d będzie minimum z tych $3i, 3j+1, 3k+2$ dla których odpowiednie $r_2, s_2, t_2 \neq 0$. Wtedy $f = x^d f'$ gdzie f' jest funkcją regularną w punkcie $(0, 0)$ c.k.d.

Przykład

$\frac{Z}{Y}$ ma zero rzędu 3 w punkcie $\Theta^* \text{ na } E^*$, Z ma zero rzędu 3 na E gdyż $Z = x^3 r, r(0,0) \neq 0$.

Zatem $\frac{Y}{Z}$ i $\frac{1}{Z}$ mają bieguny rzędu 3 w $(0, 0)$ ponieważ $\text{ord}_p\left(\frac{X}{Y}\right) = 1$

więc $\frac{x-xZ}{Z} = \frac{\frac{X-xZ}{Y} * Y}{Z}$ ma biegun rzędu 2 w punkcie $0^* \in E^*$.

Wcześniej pokazaliśmy jakie zera (i rzędy zer) ma funkcja liniowa

$\frac{X-x}{Z}$. Teraz w przestrzeni rzutowej ujednorodnienie funkcji $\frac{X-x}{Z}$ to $\frac{X}{Z} - x = \frac{X-xZ}{Z}$. W tym przypadku widać, że suma rzędów zer i biegunów jest równy 0.

5.3 Grupa dywizorów

Dla kontrolowania rzędów zer i biegunów funkcji wymiernych wygodnie jest haszować je jako współczynniki grupy abelowej wolnej generowanych przez punkty krzywej E .

Przykład

Niech $P=(x, y) \in E$ E - krzywa afiniczna

mamy przypadki:

1) Jeśli $p=(x, y)$ nie jest punktem rzędu 2 (tzn. $y \neq \bar{y}$) to funkcja $X-x$ jest parametrem lokalnym i ma zera w punktach $p=(x, y)$, $\bar{p}=(x, \bar{y})$ oraz 0 rzędu zero w dowolnym innym punkcie krzywej E .

2) $\text{char} \neq 2$ i P jest punktem rzędu 2 na E i założmy, że E jest w postaci normalnej $Y^2=(X-x_1)(X-x_2)(X-x_3)$ gdzie x_1, x_2, x_3 - różne.

Ponieważ Y jest parametrem lokalnym to $X-x_1$ ma zero rzędu 2 w punkcie $P_1=(x_1, y_1)$ i zera rzędu zero we wszystkich pozostałych punktach krzywej. Podobnie $x=x_2$ i $x=x_3$

3) $\text{char} K=2$, p jest punktem rzędu 2 na E wtedy sprowadzając E do postaci normalnej mamy $E: Y^2 + xY = X^3 + a_2X^2 + a_6$ i parametrem lokalnym jest $Y + \sqrt{a_6}$ gdyż $X = (Y + \sqrt{a_6})^2 \frac{1}{X^2 + a_2X + Y}$

Zatem funkcja X ma zero podwójne w punkcie $p=(0, \sqrt{a_6})$ i zerem rzędu zero we wszystkich pozostałych punktach.

Definicja

Grupę abelową generowaną przez punkty krzywej E nazywamy grupą dywizorów krzywej E .

$$\text{Div}(E) = \sum_{P \in E} m_P(P) \quad \text{gdzie} \quad m_P = 0 \quad \text{dla prawie wszystkich punktów} \quad P \in E.$$

Działanie dodawania dywizorów wygląda następująco:

$$\Delta_1 = \sum m_P(P) \quad \Delta_2 = \sum m_{P'}(P)$$

$$\Delta_1 + \Delta_2 = \sum (m_P + m_{P'})(P)$$

Definicja

Stopień dywizora $\Delta \in \text{Div}(E)$ tożsamość $\deg \Delta = \sum_{P \in E} m_P$

Podgrupę dywizorów stopnia 0 nazywamy $\text{Div}^0(E)$

Definicja

Dywizorem głównym nazywamy (dywizor funkcji r) dywizor postaci

$$\text{Div} r = \sum \text{ord}_P r(P) \quad \text{gdzie} \quad r \in K(E)$$

W dalszym ciągu udowodnimy że dywizory główne stanowią podgrupę grupy $Div(E)$

Pokazaliśmy, że funkcja wymierna $r = \frac{X-x^2}{Z}$ ma dwa zera (licząc w krotnościach) i jeden bigun rzędu 2 w nieskończoności na krzywej rzutowej E^* . To oznacza, że $P=(x,y,1) \in E^*$ jest reprezentantem klasy $[X, Y, Z]$, natomiast $\bar{P}=(x_3, -y-a_1x-a_3)$.

Izomorfizm krzywych $\psi: E \rightarrow E^*$ indukuje odpowiedni izomorfizm ciała frunkcji wymiernych $\psi: K(E) \rightarrow K(E^*)$ $r \rightarrow \psi(r) := r \circ \psi$.

W szczególności więc izomorfizm odpowiednich pierścieni lokalnych

$\psi: \theta_P(E) \rightarrow \theta_{\phi(P)}(E')$ a zatem i grup dywizonów $\psi: Prin(E) \rightarrow Prin(E')$ zadanych wzorem $div(\psi(r)) = div(r \circ \psi) = \psi(div r) = \sum ord_{\phi(P)}(r \circ \psi)(\psi(P))$

Odwzorowanie $div: K(E)^* \rightarrow Div(E)$ zadana wzorem

$div(r) = \sum ord_P(r)(P)$ jest homorfizmem grupy gdyż $ord_P(r_1, r_2) = ord_P(r) + ord_P(r_2)$. Szczególnym izomorfizmem jest sprzężenia który jest inwolucja, a więc $(\psi = \phi)$. Stąd mamy, że $div(\psi(r)) = div(r \circ \psi) = div(\bar{r})$ oraz $\phi(dir(r)) = \psi(dir(r)) = dir(r)$ tj. $dir(\bar{r}) = dir(r)$.

Uwaga

Korzystając z faktu, że dowolna funkcja wielomianowa $f \in K[E]$ ma stopień $N(f)$ zer (licząc z krotnościami), dowodzi się że f^* ma biegun rzędu $\max(2 st.v, 2 st.w + 3)$ w punkcie skończonym gdzie $f = v(x) + Yw(X)$.

Wniosek

Jeśli $f = v(X) + Yw(x) \in K[E]$ to $st.N(f) = \max(2 st.v, 2 st.w)$

Dowód

$N(f) = v^2 + N(Y)w^2 + Tr(Y)w \cdot v$ gdzie $st.Tr(Y)w \leq 1 + st.w < + 2st.w$
 $st.N(T) = st(Y \cdot \bar{Y}) = st.(x^3 + a_4 X^2 + a_6) = 3$ c.k.d

Ponieważ powyższe maximum jest co najmniej równe 2 otrzymujemy

Wniosek 1

Każde niestałe funkcje $f \in K(E)$ ma co najmniej 2 zera (liczone z

krotnościami)

Wniosek 2

Funkcja wymierna $r \in K(E^*)$ ma tyle zer co biegunów.

Wiemy, że ujednorodnienie wielomianu $f \in K[E]$ może mieć biegun w punkcie nieskończonym ale nie w punkcie skończonym. Odwrotnie zachodzi.

Lemat

Jeśli $r \in K(E)$ nie ma biegunów w punktach skończonych to r_* jest wielomianem.

Z powyższych uwag wynika stwierdzenie :

Funkcja wymierna należąca do $K(E)$ zadająca dywizor główny jest wyznaczona jednoznacznie z dokładnością do stałej $\neq 0$.

5.4 Grupa Picarda

Definicja

Grupą Picarda krzywej eliptycznej E nazywamy grupę ilorazową

$$Pic(E) = \frac{Div(E)}{Prin(E)}$$
 (mierzymy odstępstwo grupy dywizorów od grupy dywizorów głównych).

Część zerowa grupy Picarda to grupa ilorazowa

$$Pic^0(E) = \frac{Div(E)}{Prin(E)}$$

która jest izomorficzna z grupą punktów wymiernych na krzywej eliptycznej

$E/K \simeq Div^0(E)/Prin(E)$. Zatem, każdy punkt P na krzywej E będziemy identyfikować z dywizorem $(P) - (Q)$ stopnia 0 z dokładnością do dywizorów głównych. Co więcej $A = \sum a_p(P)$ jest dywizorem głównym, wtedy i tylko wtedy :

$$\begin{cases} \sum a_p = 0 \text{ oraz} \\ \sum a_p P = \theta \end{cases}$$

w sensie struktury grupowej na E . Dywizor główny nazywamy często - dywizorem funkcji i oznaczamy $(f) = \sum \text{ord}_P f(P)$

Dywizory funkcji liniowych

Niech $l: ax + by + c = 0$ i niech P, Q, R będą punktami przecięcia krzywej E z prostą l , wtedy $\text{Div}(l) = (P) + (Q) + (\overline{P+Q}) - 3(\theta)$

Jeśli $b=0$ to $l: x+c=0$ wtedy dywizor $\text{Div}(l^*) = (P) + (\overline{P}) - 2(\theta)$

Definicja

Jeśli f jest funkcja na krzywej E oraz $A = \sum a_p(P)$ jest dywizorem to

$$f(A) = \prod_{P \in A} f(P)^{a_p}$$

Przykład:

$$f(x, y) = x - x_R$$

$$A = (P) - (Q)$$

$$f(A) = (x_P - x_R)^1 \cdot (x_Q - x_R)^{-1} = \frac{x_P - x_R}{x_Q - x_R}$$

$$f((P) - (Q)) = f(P) \cdot f(Q)^{-1} = \frac{f(P)}{f(Q)}$$

Definicja

Dwa dywizjony Δ_1, Δ_2 nazywamy liniowo niezależnymi wtedy i tylko wtedy gdy ich warstwy modulo $\text{Prin}(E)$ są identyczne tzn. :

$$\Delta_1 \sim \Delta_2 \Leftrightarrow \Delta_1 - \Delta_2 \in \text{Prin}(E)$$

Badanie dywizorów sprowadza się do badania dywizorów funkcji liniowych tj. funkcji postaci :

$$l = \alpha X + \beta Y + \gamma \text{ gdzie } \alpha \text{ lub } \beta \neq 0.$$

Jeżeli $\beta \neq 0$ to zachodzi :

Lemat

Niech $l = Y - (mX + b)$ $P = (x, y, 1) \in E^* \cap C^*$ wtedy $\text{ord}_p l^*$ jest krotnością x jako zero wielomianu $E(X, mX + b)$

Dowód

Wystarczy przedstawić $E(X, T)$ w postaci

$$T^2 - \text{Tr}(Y)T - N(Y) = (Y - T)(\bar{Y} - T) \quad \text{oraz wykorzystać reprezentację}$$

$$E(X, mx + b) = -(X - x_1)(X - x_2)(X - x_3) = (l^*)(\tau^*)$$

gdyż

$$(l^*)(\tau^*)^* = (y - (mx + b))(\bar{Y} - mx + b) = (Y - T)(\bar{Y} - T), \quad \text{gdzie } T = mx + b$$

Z powyższego lematu można otrzymać wzory na dodanie punktów na krzywej eliptycznej.

Działania na krzywej $E(K)$

Niech $y = \alpha x + \beta$ będzie sieczną przechodzącą przez punkty $(x_1, y_1), (x_2, y_2)$ krzywej E wtedy $(\alpha x + \beta)^2 = x^3 + Ax + B$.

gdzie

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1} \quad (x_2 \neq x_1) \quad ; \quad \beta = y_2 - \alpha x_2 = y_2 - \frac{y_2 - y_1}{x_2 - x_1} * x_2$$

Ze wzorów Viète'a

$$x_1 + x_2 + x_3 = \alpha^2$$

skąd

$$(\#) \quad \begin{cases} x_3 = -x_1 - x_2 + \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 \\ y_3 = \alpha x_3 + \beta \end{cases}$$

Jeśli $x_1 = x_2$ (sieczna jest styczną) to jej równanie ma postać $y = \alpha x + \beta$ gdzie

$$\alpha = \frac{dy}{dx}$$

Ponieważ:

$$dE = \frac{\partial E}{\partial x} dx + \frac{\partial E}{\partial y} dy = 0 \quad \text{więc} \quad \frac{dy}{dx} = - \frac{\partial E / \partial x}{\partial E / \partial y}$$

$$\alpha = \frac{dy}{dx} = - \frac{\partial E / \partial x}{\partial E / \partial y} = - \frac{3x^2 + A}{2y}$$

układ (#) zachodzi z odpowiednimi wartościami α i β to mamy:

$$x_3 = -2x_1 + \left(\frac{3x_1^2 + A}{2y_1} \right)^2 = \frac{x_1^4 + 2Ax_1^2 - 8x_1B + A^2}{4(x_1^3 + Ax_1 + B)} = \frac{x_1^4 + 2Ax_1^2 - 8x_1B + A^2}{f(x_1)}$$

Zatem jeśli $y_1=0$ to $x_3=\infty$ (styczna jest pionowa) to jest $(x_3, y_3)=O$. W ten sposób określiliśmy działanie na krzywej $E(R)$. Te same wzory zadają działanie na krzywej nad dowolnym ciałem charakterystyki $\neq 2, 3$ (bo wtedy E zadaje się równaniem Weierstrassa). $y^2=f(x)$

Wniosek

$(E(K), +)$ jest grupą abelową. Przypuszczenie Poincare (1900 r.) mówi, że dla ciał liczbowych K , $(E(K), +)$ jest skończenie generowaną grupą abelową i zostało udowodnione przez Mordella w 1928 r.. Natomiast w pełnej ogólności (dla rozmaitości abelowych) przez Weila.

Mamy: $E(K) = \mathbb{Z}' \oplus E$

(Mazur (1977 r.) udowodnił, że dla $K=\mathbb{Q}$, $E(\mathbb{Q}) = \mathbb{Z}_m$, $m = 0, 1, \dots, m$

Lub $E(\mathbb{Q}) = \mathbb{Z}_m \oplus \mathbb{Z}_2$ i wyznaczył dopuszczalne wartości m .

