

Polje $\mathbb{Q}(E[3])$ za $E: y^2 = x^3 + x^\dagger$

Tomislav Pejković

11.6.2008.

Sadržaj

1 Pregled definicija i rezultata	1
2 Točke reda 3 u $E(\mathbb{C})$	2
3 Proširenje $\mathbb{Q}(E[3])$ od \mathbb{Q}	4

1 Pregled definicija i rezultata

Podsjetimo se najprije nekih osnovnih definicija.

- ★ $E[n] = \{P \in \mathbb{C}[E] : nP = \mathcal{O}\}$.
- ★ $\mathbb{Q}(E[n]) = \left(\begin{array}{l} \text{polje generirano nad } \mathbb{Q} \text{ sa } x \text{ i } y \\ \text{koordinatama svih točaka iz } E[n] \end{array} \right)$.
- ★ Eliptička krivulja E ima kompleksno množenje ako postoji homomorfizam $\phi : E \rightarrow E$ zadan racionalnim funkcijama koji je različit od množenja s : $P \mapsto nP$ za svaki $n \in \mathbb{Z}$.

U ovom seminaru promatrat ćemo eliptičku krivulju E zadanu jednačbom $y^2 = x^3 + x$. Spomenimo i nekoliko tvrdnji vezanih uz ovu krivulju koje su dokazane u okviru predavanja i zadaća:

- Vrijedi $E[n] \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}}$ (općenito, ne samo za našu krivulju).
- $\mathbb{Q}(E[n]) = \mathbb{Q}(x_1, y_1, \dots, x_{n^2-1}, y_{n^2-1})$ je Galoisovo proširenje od \mathbb{Q} konačnog stupnja (općenito).
- Eliptička krivulja E ima kompleksno množenje $\phi(x, y) = (-x, iy)$.
- $\phi : E[n] \rightarrow E[n]$, pa je $i \in \mathbb{Q}(E[n])$.
- $\mathbb{Q}(E[n])$ je Galoisovo proširenje od $\mathbb{Q}(i)$ i $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}(i))$ je Abelova grupa.

[†]Seminar održan u okviru kolegija Uvod u aritmetiku eliptičkih krivulja.

- Svaki element $\sigma \in \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ može se na jedinstven način prikazati kao $\sigma = st$, gdje je $s \in \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}(i))$ i $t \in \{\text{id}, \tau\}$ (τ je kompleksno konjugiranje, a id je identiteta).
- Za sve $s \in \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}(i))$ je $s\tau = \tau s^{-1}$.
- $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ je Abelova ako i samo ako svaki $s \in \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}(i))$ zadovoljava $s^2 = \text{id}$.

Za krivulju E dokazani su i sljedeći konkretni rezultati za $n = 2$ i $n = 4$.

- $E[2] = \{\mathcal{O}, (0, 0), (i, 0), (-i, 0)\}$, pa je $\mathbb{Q}(E[2]) = \mathbb{Q}(i)$ i $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = \{\text{id}, \tau\}$.

-

$$E[4] = \{\mathcal{O}\} \cup E[2] \cup \{(1, \pm\sqrt{2}), (-1, \pm i\sqrt{2}), (\alpha, \pm\beta), (-\alpha, \pm i\beta), (\alpha^{-1}, \pm\alpha^{-2}\beta), (-\alpha^{-1}, \pm i\alpha^{-2}\beta)\},$$

gdje je $\alpha = (\sqrt{2} - 1)i = -i + i\sqrt{2}$ i $\beta = (1 + i)(\sqrt{2} - 1) = -1 - i + \sqrt{2} + i\sqrt{2}$. Zato je $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt{2})$ i $\text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) = \{\text{id}, \sigma, \tau, \sigma\tau\} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$, gdje je σ zadano na generatorima sa $\sigma(i) = i$, $\sigma(\sqrt{2}) = -\sqrt{2}$.

U ostatku izlaganja proučavat ćemo $\text{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$.

2 Točke reda 3 u $E(\mathbb{C})$

Ako je $P = (x, y)$ točka na krivulji E : $y^2 = x^3 + x$, onda je

$$2P = \left(\frac{x^4 - 2x^2 + 1}{4y^2}, \frac{x^6 + 5x^4 - 5x^2 - 1}{8y^3} \right)$$

Prethodnu formulu dokazujemo standardnim postupkom. Neka je $P = (x_P, y_P)$ na E . Tada je

$$\begin{aligned} y^2 &= f(x) = x^3 + x \\ 2yy' &= f'(x) \quad \Rightarrow \quad \lambda = y'_P = \frac{f'(x_P)}{2y_P} = \frac{3x_P^2 + 1}{2y_P}. \end{aligned}$$

Tangenta na E u točki (x_P, y_P) ima jednadžbu

$$y - y_P = \lambda(x - x_P)$$

i siječe E u točki koja je rješenje od

$$\begin{aligned} &\begin{cases} y^2 = x^3 + x \\ y = \lambda x - \lambda x_P + y_P \end{cases} \\ \Rightarrow &x^3 + x = (\lambda x - \lambda x_P + y_P)^2 \\ &x^3 - \lambda^2 x^2 + (1 - 2\lambda(-\lambda x_P + y_P))x - (\lambda x_P - y_P)^2 = 0 \end{aligned}$$

Dvostruki korijen ovog polinoma je x_P , a treći korijen je upravo x koordinata točke $2P$, pa je zbog Vièteovih formula

$$2x_P + x_{2P} = \lambda^2 = \left(\frac{3x_P^2 + 1}{2y_P} \right)^2$$

$$\Rightarrow x_{2P} = \frac{9x_P^4 + 6x_P^2 + 1}{4y_P^2} - \frac{8x_P(x_P^3 + x_P)}{4y_P^2} = \frac{x_P^4 - 2x_P^2 + 1}{4y_P^2}.$$

Točke (x_P, y_P) i $(x_{2P}, -y_{2P})$ leže na prije spomenutoj tangenti s koeficijentom smjera λ , pa je

$$\frac{-y_{2P} - y_P}{x_{2P} - x_P} = \lambda = \frac{3x_P^2 + 1}{2y_P}, \quad \text{tj.}$$

$$y_{2P} = - \left(\frac{3x_P^2 + 1}{2y_P} (x_{2P} - x_P) + y_P \right)$$

$$= - \left(\frac{(3x_P^2 + 1)(x_P^4 - 2x_P^2 + 1)}{8y_P^3} - \frac{4x_P y_P^2 (3x_P^2 + 1)}{8y_P^3} + \frac{8y_P^4}{8y_P^3} \right)$$

$$= [y_P^2 = x_P^3 + x_P] = \frac{x_P^6 + 5x_P^4 - 5x_P^2 - 1}{8y_P^3}.$$

Primjetimo da je

$$P = (x, y) \text{ točka reda } 3 \Leftrightarrow 3P = \mathcal{O} \text{ i } P \neq \mathcal{O}$$

$$\Leftrightarrow 2P = -P \text{ i } P \neq \mathcal{O}$$

$$\Leftrightarrow (x_{2P}, y_{2P}) = (x_P, -y_P)$$

$$\Leftrightarrow x_{2P} = x_P$$

$(x_{2P} = x_P$ povlači da je $2P = P$ ili $2P = -P$,
prva mogućnost otpada jer bi bilo $P = \mathcal{O}$)

$$\Leftrightarrow \frac{x^4 - 2x^2 + 1}{4y^2} = x$$

$$\Leftrightarrow 3x^4 + 6x^2 - 1 = 0 \text{ jer je } y^2 = x^3 + x.$$

Dakle, točke reda tri u $E(\mathbb{C})$ su točke kojima x koordinata zadovoljava jednadžbu

$$3x^4 + 6x^2 - 1 = 0.$$

Sada svaki od x -eva daje dvije moguće vrijednosti za y (točke u kojima je $y = 0$ su reda dva, a ne tri). Tako dobivamo osam točaka reda tri koje zajedno s \mathcal{O} čine grupu

$$E[3] \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

Riješimo prije spomenutu jednadžbu eksplicitno (to je bikvadratna jednadžba)

$$3x^4 + 6x^2 + 1 = 3\left(x^4 + 2x^2 + 1 - \frac{4}{3}\right) = 3\left((x^2 + 1)^2 - \frac{4}{3}\right)$$

$$= 3\left(x^2 + 1 - \frac{2\sqrt{3}}{3}\right)\left(x^2 + 1 + \frac{2\sqrt{3}}{3}\right)$$

$$= 3\left(x^2 - \frac{2\sqrt{3} - 3}{3}\right)\left(x^2 + \frac{2\sqrt{3} + 3}{3}\right)$$

$$= 3\left(x - \sqrt{\frac{2\sqrt{3} - 3}{3}}\right)\left(x + \sqrt{\frac{2\sqrt{3} - 3}{3}}\right)\left(x - i\sqrt{\frac{2\sqrt{3} + 3}{3}}\right)\left(x + i\sqrt{\frac{2\sqrt{3} + 3}{3}}\right).$$

Stavimo li $\alpha := \sqrt{\frac{2\sqrt{3}-3}{3}}$, vidimo da su korijeni

$$\alpha, -\alpha, \frac{1}{i\sqrt{3}\alpha}, -\frac{1}{i\sqrt{3}\alpha}.$$

Uvrstimo li ih u $y^2 = x^3 + x$, dobivamo y -koordinate traženih točaka. Neka je

$$\beta = \sqrt{\alpha^3 + \alpha} = \sqrt{\alpha(\alpha^2 + 1)} = \sqrt{\frac{2\alpha}{\sqrt{3}}} = \sqrt[4]{\frac{8\sqrt{3}-12}{9}}.$$

Tada je devet točaka iz $E[3]$ upravo

$$E[3] = \{\mathcal{O}, (\alpha, \pm\beta), (-\alpha, \pm i\beta), \left(\frac{i}{\sqrt{3}\alpha}, \pm \frac{2\sqrt{-i}}{\sqrt[4]{27}\beta}\right), \left(\frac{-i}{\sqrt{3}\alpha}, \pm \frac{2\sqrt{i}}{\sqrt[4]{27}\beta}\right)\}.$$

Primjerice

$$\begin{aligned} \left(\frac{i}{\sqrt{3}\alpha}\right)^3 + \frac{i}{\sqrt{3}\alpha} &= \frac{-i}{3\sqrt{3}\alpha^3} + \frac{i}{\sqrt{3}\alpha} = \frac{i}{\sqrt{3}\alpha} \left(-\frac{1}{3\alpha^2} + 1\right) \\ &= \frac{i}{\frac{\sqrt{3}\sqrt{3}\beta^2}{2}} \left(-\frac{1}{3 \cdot \frac{2\sqrt{3}-3}{3}} + 1\right) = \frac{2i}{3\beta^2} \left(\frac{-(2\sqrt{3}+3)}{(2\sqrt{3})^2 - 3^2} + 1\right) \\ &= \frac{2i}{3\beta^2} \cdot \frac{-2\sqrt{3}}{3} = \frac{-4i}{3\sqrt{3}\beta^2} = \left(\frac{2\sqrt{-i}}{\sqrt[4]{27}\beta}\right)^2. \end{aligned}$$

3 Proširenje $\mathbb{Q}(E[3])$ od \mathbb{Q}

Polje generirano koordinatama točaka iz $E[3]$ je

$$\begin{aligned} \mathbb{Q}(E[3]) &= \mathbb{Q}\left(\alpha, \beta, i, \sqrt{3}, \frac{\sqrt{-i}}{\sqrt[4]{27}}\right) \\ &= \left[\begin{array}{l} \beta = \sqrt[4]{\frac{8\sqrt{3}-12}{9}} \Rightarrow \sqrt{3} = \frac{9\beta^4 + 12}{8} \\ \beta = \sqrt{\frac{2\alpha}{\sqrt{3}}} \Rightarrow \alpha = \frac{\beta^2\sqrt{3}}{2} = \frac{9\beta^6 + 12\beta^2}{16} \\ \frac{\sqrt{-i}}{\sqrt[4]{27}} = \frac{\pm\left(\frac{i-1}{\sqrt{2}}\right)}{\sqrt[4]{27}} = \pm \frac{i-1}{2} \cdot \frac{\sqrt{2}}{\sqrt[4]{27}} = \pm \frac{i-1}{2} \cdot \frac{\beta^2(1+\sqrt{3})}{2} \\ \qquad \qquad \qquad = \pm \frac{i-1}{2} \cdot \frac{\beta^2(9\beta^4 + 20)}{16}. \end{array} \right] \\ &= \mathbb{Q}(\beta, i). \end{aligned}$$

Potražimo sada minimalni polinom od β nad $\mathbb{Q}(\mathbb{Q}(i))$.

$$\begin{aligned} \beta = \sqrt[4]{\frac{8\sqrt{3}-12}{9}} &\Rightarrow \beta^4 = \frac{8\sqrt{3}-12}{9} \Rightarrow 9\beta^4 + 12 = 8\sqrt{3} \\ &\Rightarrow (9\beta^4 + 12)^2 = 64 \cdot 3 \Rightarrow 81\beta^8 + 216\beta^4 + 144 = 192 \\ &\qquad \qquad \qquad \Rightarrow 27\beta^8 + 72\beta^4 - 16 = 0 \end{aligned}$$

Polinom $p(x) = 27x^8 + 72x^4 - 16$ faktorizirajmo

$$p(x) = 27x^8 + 72x^4 - 16$$

$$= \left[\begin{array}{l} p(x) = 0 \Leftrightarrow 9x^4 + 12 = \pm 8\sqrt{3} \Leftrightarrow x^4 = \frac{\pm 8\sqrt{3} - 12}{9} \\ \beta^4 = \frac{8\sqrt{3} - 12}{9} \\ \sqrt[4]{\frac{8\sqrt{3} - 12}{9}} = [\text{u kompleksnom smislu}] = \pm\beta, \pm i\beta \\ \frac{1}{\beta^4} = \frac{9}{8\sqrt{3} - 12} = \frac{9(8\sqrt{3} + 12)}{48} = \frac{27}{16} \cdot \frac{8\sqrt{3} + 12}{9} \\ \sqrt[4]{\frac{-8\sqrt{3} - 12}{9}} = \sqrt[4]{-\frac{16}{27} \cdot \frac{1}{\beta^4}} = \frac{2}{\sqrt[4]{27}} \cdot \frac{\pm\sqrt{\pm i}}{\beta} \\ = \pm(i-1)\frac{\beta(9\beta^4 + 20)}{16}, \pm i(i-1)\frac{\beta(9\beta^4 + 20)}{16} \end{array} \right]$$

$$= \left[\text{uvodimo oznaku } b := (i-1)\frac{\beta(9\beta^4 + 20)}{16} \right]$$

$$= 27(x - \beta)(x + \beta)(x - i\beta)(x + i\beta)(x - b)(x + b)(x - ib)(x + ib).$$

Kombiniranjem linearnih faktora u rastavu od $p(x)$ ne možemo dobiti polinom nad \mathbb{Q} , pa je p ireducibilan nad \mathbb{Q} . (štoviše i nad $\mathbb{Q}(i)$).

Ako sa σ označimo automorfizam polja $\mathbb{Q}(\beta, i)$ tako da je

$$\sigma(\beta) = b = (i-1)\frac{\beta(9\beta^4 + 20)}{16}, \quad \sigma(i) = i,$$

a sa τ kompleksno konjugiranje, onda je djelovanje od σ i τ na korijenima od p dano sa

hom.	djelovanje na korijene							
id	β	$-\beta$	$i\beta$	$-i\beta$	b	$-b$	ib	$-ib$
	1	5	3	7	2	6	4	8
σ	b	$-b$	ib	$-ib$	$i\beta$	$-i\beta$	$-\beta$	β
	2	6	4	8	3	7	5	1
τ	β	$-\beta$	$-i\beta$	$i\beta$	ib	$-ib$	b	$-b$
	1	5	7	3	4	8	2	6

Numeriranjem korijena dobili smo ulaganje Galoisove grupe $\iota : \text{Gal}(\mathbb{Q}(\beta, i)/\mathbb{Q}) \hookrightarrow S_n$ u simetričnu grupu stupnja n (sadrži sve permutacije skupa $\{1, \dots, n\}$, prikazivat ćemo ih rastavom na cikluse), pri čemu je $\sigma \mapsto (12345678)$ (zato tako neobična numeracija) i $\tau \mapsto (1)(24)(37)(5)(68)$. Nije teško vidjeti da je

$$\sigma\tau = \iota^{-1}((1256)(3874)) = \tau\sigma^3$$

i da su svi elementi

$$\sigma^k\tau^j, \quad k = 0, 1, \dots, 7, \quad j = 0, 1$$

različiti, pa budući da je

$$|\mathrm{Gal}(\mathbb{Q}(\beta, i)/\mathbb{Q})| = [\mathbb{Q}(\beta, i) : \mathbb{Q}] = [\mathbb{Q}(\beta, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 8 \cdot 2 = 16,$$

zaključujemo da je naša grupa generirana sa σ, τ . Dakle, ova grupa reda 16 ima prezentaciju

$$\langle \sigma, \tau \mid \sigma^8 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle.$$

Primjetimo da ovo nije takozvana diedralna grupa (!!!):

$$\langle \sigma, \tau \mid \sigma^8 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$$

u što se možemo uvjeriti i tako da vidimo da naša grupa, koja se u literaturu naziva i kvazidiedralna ili semidiedralna ima samo 5 elemenata reda 2, dok diedralna grupa ima 9 elemenata reda 2.

Literatura

- [G] Gusić, I. – *Uvod u aritmetiku eliptičkih krivulja*. bilješke s predavanja na poslijediplomskom studiju, Zagreb, 2008.
<http://web.math.hr/~duje/seminar.html>
- [ST] Silverman, Joseph H.; Tate, John. – *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.
- [W] Wild, Marcel. – *The groups of order sixteen made easy*. Amer. Math. Monthly **112** (2005), no. 1, 20–31.