

אלגברה ב2

© ארזים

20 ביוני 2017

1 עקומים אליפטיים

בשיעור הקודם הגדרנו את פעולת החיבור ואת האפס, O , של $E(K)$.

תכונות

$$1. P + O = O + P = P$$

$$2. P + (-P) = O$$

$$3. P + (Q + R) = (P + Q) + R$$

$$4. P + Q = Q + P$$

תכונות אלה הופכות את $E(K)$ לחבורה אבלית. תכונות 1,2,4 טריוויאליות - 3 ממש קשה להוכחה (נוותר על זה). יש הוכחות של זה עם אלגברה מתקדמת, ועם אנליזה מתקדמת (מרוכבות 2).

דוגמא ניקח את $E: y^2 = x^3 - 5x + 8$, וניקח $P = (1, 2)$. אזי

$$2P = P + P = \left(-\frac{7}{4}, -\frac{27}{8}\right)$$

$$3P = 2P + P = \left(\frac{553}{121}, -\frac{11950}{1331}\right)$$

$$4P = 2P + 2P = \left(\frac{45313}{11664}, -\frac{8655103}{1259712}\right)$$

כעת נחשב נוסחה עבור חוק החיבור:

$$y^2 = x^3 + Ax + B$$

$$P_1 = (x_1, y_1)$$

$$P_2 = (x_2, y_2)$$

השיפוע של הקו שיש להעביר הוא

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P_1 \neq P_2 \\ \frac{3x_1^2 + A}{2y_1} & P_1 = P_2 \end{cases}$$

ואז הישר הוא

$$L : y = \lambda x + \nu$$

כאשר ν מתאים $(\lambda x_1 + y_1)$ למשל. נמצא את הנקודה השלישית $P_3 = (x_3, y_3)$ על הישר ועל העקום:

$$\begin{aligned}(\lambda x + 3)^2 &= x^3 + Ax + B \\ x^3 + Ax + B - (\lambda x + \nu)^2 &= (x - x_1)(x - x_2)(x - x_3)\end{aligned}$$

נשווה את המקדם של x^2 :

$$\begin{aligned}-\lambda^2 &= -(x_1 + x_2 + x_3) \\ x_3 &= \lambda^2 - x_1 - x_2\end{aligned}$$

ואז

$$y_3 = \lambda x_3 + \nu$$

ולכן בסך הכל

$$P_1 + P_2 = (x_3, -y_3)$$

נחלק למקרים עבור הצגות קונקרטיות יותר:

1. אם $P_1 \neq P_2, x_1 = x_2$ אז $P_1 + P_2 = O$.
2. אם $P_1 = P_2, x_1 = 0$ אז $P_1 + P_2 = O$.
3. אם $P_1 \neq P_2, x_1 \neq x_2$ אז $\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$ ואז מציבים.
4. אם $P_1 = P_2, y_1 \neq 0$ אז $\lambda = \frac{3x_1^2 + A}{2y_1}, \nu = \frac{-x_1^3 + Ax_1 + 2B}{2y_1}$ ואז מציבים.

אפשר לפשט קצת (נוותר), אבל מכאן אנחנו רואים שאם A, B, P, Q מוגדרים מעל שדה K , אז גם $P + Q$ מוגדר מעל K , ולכן $E(K) \cup \{O\}$ חבורה אבלית.

משפט 1.1 (פואנקרה) אם $A, B \in K, K \subseteq L$ אזי $E(K) \leq E(L)$.

נרצה להבין איך $E(K)$ נראית (כמובן שזה תלוי בשדה K). תמיד נכתוב $E(K)$ ונניח שהוא מכיל כבר את O . את $E(\mathbb{R})$ כבר ראינו. כעת נדון במקרה $E(\mathbb{C})$. בשביל זה נגדיר שריג:

הגדרה 1.2 השריג שנוצר על ידי $\omega_1, \omega_2 \in \mathbb{C}$ בלתי תלויים לינארית מעל $\mathbb{R}$ הוא $\mathcal{L}(\omega_1, \omega_2) = \{a_1 \omega_1 + a_2 \omega_2 \mid a_1, a_2 \in \mathbb{Z}\}$.

נשים לב שאם ניקח $\mathbb{C}/\mathcal{L}$ נקבל את $\mathbb{T}$, טורוס, שהוא גם $S_1 \times S_1$. מסתבר (שוב מרוכבות 2) שההעתקה

$$\begin{aligned}\mathbb{C}/\mathcal{L} &\rightarrow E(\mathbb{C}) \\ w + \mathcal{L} &\rightarrow \left(p(w), \frac{1}{2} p'(w) \right)\end{aligned}$$

היא איזומורפיזם של חבורות, כאשר p פונקציית ויירשטראס:

$$p(z) = \frac{1}{z^2} + \sum_{0 \neq w \in \mathcal{L}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

שמקיימת את המשוואה הדיפרנציאלית

$$\left(\frac{1}{2}p'(w)\right)^2 = p(w)^3 + Ap(w) + B$$

ולכן זו אכן על העקום. כעת נחפש את נקודות הפיתול (נקודות מסדר סופי) על $E(\mathbb{C})$. נקודות פיתול מסדר N על S_1 הן $S_1 = \{|z|=1\} \subseteq \mathbb{C}$ הן $\mu_n \subseteq \mathbb{Z}/n\mathbb{Z} \cong \mu_n$. לכן נקודות הפיתול על $E(\mathbb{C})$ הן

$$E(\mathbb{C})[N] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

כאשר

$$G[N] = \{g \in G \mid g^N = 1\}$$

כאשר G אבלית.