

אלגברה ב2

© ארזים

20 ביוני 2017

1 עקומים אליפטיים

יהי E עקום אליפטי. נעבוד עם

$$E := y^2 = x^3 + x/c$$

במקרה זה $E \cong \mathbb{C}/\mathbb{Z}[i]$. נגדיר $\text{End}_{\mathbb{C}}(E)$ את חוג הפונקציות הרציונליות מהעקום לעצמו (כל אחת כזו היא בפרט הומומורפיזם של החבורה של העקום). יש למשל את

$$(x, y) \rightarrow (x, -y)$$
$$m(x, y) = \underbrace{(x, y) + \dots + (x, y)}_m$$

ולכן

$$\mathbb{Z} \subseteq \text{End}(E)$$

יש גם חיבור של אנדומורפיזמים, בגלל החיבור בעקום, ולכן זהו אכן חוג (הכפל הוא הרכבה).

תרגיל מצאו אוטומורפיזם מסדר 4 של E .

פתרון

$$(x, y) \mapsto (-x, iy) \mapsto (x, -y)$$

ולכן $(x, y) \rightarrow (-x, iy)$ עובד.

תרגיל ניקח $p \equiv 1 \pmod{4}$ אזי

$$|E(\mathbb{F}_p)| = 0 \pmod{4}$$

פתרון יש שורש של -1 מודולו p , מההנחה עליו, ולכן אותו אוטומורפיזם λ מלפני רגע עדיין קיים (i הוא שורש כלשהו של -1). הנקודות כאן מתחלקות לרביעיות, מסלולים תחת האוטומורפיזם הזה, פרט לאלה שמקיימות $\lambda^2(P) = P$. נבדוק מתי זה מתקיים:

$$\lambda^2(x, y) = (x, -y) = (x, y) \iff y = 0 \iff x^3 + x = 0 \iff (x, y) \in \{(0, 0), (i, 0), (-i, 0)\}$$

ויש גם את הנקודה באינסוף. לכן האיברים עדיין ברביעיות.

טענה 1.1 (שלא נוכיח) החוג $\text{End}_{\mathbb{C}}(E)$ הוא קומוטטיבי.

תרגיל אם $p \neq 1$ אז $\text{End}_{\overline{\mathbb{F}}_p}(E)$ אינו קומוטטיבי (כאשר E הספציפי שלנו).

פתרון נסמן λ את האנדומורפיזם מקודם, וכן F את פרובניוס:

$$F(x, y) = (x^p, y^p)$$

זה עובד כי זה אוטומורפיזם גלואה. כעת,

$$\lambda F(x, y) = (-x^p, iy^p)$$

$$F\lambda(x, y) = (-x^p, -iy^p)$$

(כאן i הוא איבר מהסגור האלגברי מסדר 4).

כעת, לכל $\varphi \in \text{End}(E)$ נגדיר

$$E[\varphi] = \ker \varphi$$

בפרט, עבור $\varphi = m \in \mathbb{Z}$ (כפל פי m), נקבל בדיוק את הנקודות מסדר m :

$$E[m] = \{P \in E(\overline{\mathbb{F}}) \mid mP = O\}$$

תחת האנלוגיה הטבעית

$$E \leftrightarrow \overline{\mathbb{F}}^*$$

נקבל שנקודות פיתול מתאימות לשורשי יחידה. ניקח כעת p ראשוני, ואז האיברים מסדר p הם $(\mathbb{Z}/p\mathbb{Z})^2$, בעוד בתוך $\overline{\mathbb{F}}^*$ הם $\mathbb{Z}/p\mathbb{Z}$. כעת, החבורה $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ פועלת על שורשי היחידה מסדר p . זה נותן הומומורפיזם

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \rightarrow (\mathbb{Z}/p\mathbb{Z})^* \cong \text{GL}_1(\mathbb{Z}/p\mathbb{Z})$$

בהתאמה לעקומים אליפטיים נקבל העתקה דומה:

$$\text{Gal}(L/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

עבור L שהוא השדה הנוצר מעל \mathbb{Q} על ידי הקואורדינטות של נקודות הפיתול מסדר p של E . זוהי **הצגה** (ובגלל שהיא מחבורת גלואה, היא נקראת גם הצגת גלואה). יתר על כן:

משפט 1.2 (סר - Serre) יהי E עקום אליפטי שהשריג המתאים לו אינו מוכל בהרחבה ריבועית של \mathbb{Q} . אזי לכל p גדול מספיק, ההעתקה

$$\text{Gal}(L/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

היא על.