

אלגברה ב2

© ארזים

21 ביוני 2017

1 עקומים אליפטיים

דיברנו על העקומים $E = \{y^2 = f(x)\}$, $\deg f = 3$, $\gcd(f', f) = 1$. דיברנו על זה ספציפית מעל $\mathbb{C}$ וראינו

$$E(\mathbb{C}) \cong S^1 \times S^1 = \mathbb{T}^2$$

ומכאן קיבלנו

$$(E(\mathbb{C}))[N] = \{g \in E(\mathbb{C}) \mid g^N = 1\} \cong (\mathbb{Z}/N\mathbb{Z})^2$$

1.1 משפט פרמה האחרון

פיתגורס דיבר על שלישיות $x^2 + y^2 = z^2$, כאשר $x, y, z > 0$ שלמים. למשל, 3, 4, 5 פתרון. פרמה התעסק במשוואת פרמה:

$$x^n + y^n = z^n$$

עבור $n > 2$. פרמה, בשנת 1637, שיער שאין פתרונות, והוכיח עבור $n = 4$. הוא טען שההוכחה שלו יכולה לעבור הכללה לכל n , אבל את ההוכחה שלו הוא כתב בשולי הספר שהוא קרא, ובמילותיו, הוא לא יכול היה לתת את ההכללה כי "שוליים אלו צרים מלהכיל אותה". בשנת 1753 אוילר הוכיח את המקרה $n = 3$. בשנת 1800 לערך, סופיה ג'רמיין הראתה שאם $n \nmid x, y, z$ אז אין פתרון עבור $n < 100$. בשנת 1825 דיריכלה ולז'נדר הוכיחו את $n = 5$, ולאחר מכן למה (Lame) הוכיח את $n = 7$. בשנת 1847, קומר הוכיח עבור ראשוניים מסוימים אחרים. באיזשהו שלב מחשבים נכנסו לתמונה ובדקו את כל האפשרויות עד $4 \cdot 10^6$. בשנת 1993, המתמטיקאי הבריטי סר אנדרו ויילס (Sir Andrew Wiles) הוכיח את המשפט במקרה הכללי - בעזרת אבחנה של גרהארד פריי משנת 1984, שקישרה בין המשפט האחרון של פרמה לבין עקומים אליפטיים. כדי להוכיח את המשפט האחרון, די להוכיח עבור כל $n = p > 2$ ראשוני אי זוגי. נניח שהיה פתרון, a, b, c , עם $\gcd(a, b, c) = 1$ (בלי הגבלת הכלליות - היינו מוציאים גורמים משותפים). פריי התבונן בעקום האליפטי הבא:

$$E_{a,b,c}: y^2 = x(x - a^p)(x + b^p)$$

לעקום הזה יש תכונות "מוזרות", ולכן (בסופו של דבר הצליחו להראות) הוא לא קיים. ז'אן-פיייר סר (Jean-Pierre Serre), בשנת 1987, קישר את זה להשערה על מודולריות של E .

ריבט (Ribet), בשנת 1990, הוכיח שהשערת המודולריות של סר גוררת את המשפט האחרון של פרמה. וויילס עבד קשה והצליח לבסוף להוכיח את המשפט - בשנת 1993 הייתה הוכחה אבל לא שלמה, ולבסוף הכל תם והושלם במאמר שלו ושל התלמיד שלו, טיילור (Taylor), בשנת 1995. אנחנו נדבר כעת קצת על הנושאים הרלוונטיים.

1.1.1 הצגות גלואה, תבניות מודולריות, עקומים מודולריים ועוד

יש לנו העקום האליפטי $E: y^2 = x^3 + Ax + B$, כאשר $A, B \in \mathbb{Q}$. אז ראינו

$$E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$$

נשים לב שהקואורדינטות של $(x, y) \in E[2]$ הן אלגבריות מעל $\mathbb{Q}$, שכן $y = 0$, $f(x) = 0$. זה נכון גם לנקודות פיתול מכל סדר. בעצם, המשוואה $NP = 0$ מגדירה משוואה אלגברית מעל $\mathbb{Q}$, שאותה x_1 מקיים. לכן x_1 אלגברי, ולכן גם y_1 . נתבונן אם כן בשדה $\mathbb{Q}(E[q])$, עבור q ראשוני. יש לנו מגדיר

$$\mathbb{Q} \subseteq \mathbb{Q}(E[q]) \subseteq L$$

כאשר L הוא סגור גלואה של ההרחבה $\mathbb{Q}(E[q])/\mathbb{Q}$. יהי $P \in E[q]$ - אזי $qP = 0$. תנאי זה שקול לכך שהקואורדינטות x_1, y_1 של P מקיימות משוואה ספציפית עם מקדמים בתוך $\mathbb{Q}$. לכן, לכל $\sigma \in \text{Gal}(L/\mathbb{Q})$ יתקיים גם

$$\sigma(P) = (\sigma x_1, \sigma y_1) \in E[q]$$

כי הקואורדינטות יקיימו את אותה משוואה (שיכון גלואה). מכאן נובע כי ההרחבה $\mathbb{Q}(E[q])/\mathbb{Q}$ גלואה, ויש מונומורפיזם

$$\rho_q: \text{Gal}(\mathbb{Q}(E[q])/\mathbb{Q}) \rightarrow \text{Aut}(E[q]) \cong \text{GL}_2(\mathbb{F}_q)$$

העתקה זו נקראת הצגת גלואה מודולו q .

מסקנה 1.1 $E[q] \subseteq \mathbb{Q}$ אם ורק אם $\rho_q = 1$.

השערה (סר) כל הצגת גלואה היא "מודולרית".

משפט 1.2 (ריבט) העקום של פריי הוא לא מודולרי.

וויילס הוכיח את ההשערה, וקיבל את המשפט האחרון של פרמה כתוצאה.

2 חבורות גלואה אינסופיות

דיברנו על הרחבות גלואה, החבורות שלהן, ועל המשפט היסודי - שמבטיח התאמה חד-חד-ערכית ועל בין השריגים של תתי חבורות ושל תתי הרחבות, שהופכת סדר, שומרת אינדקסים וכן הלאה. אפשר להגדיר הרחבת גלואה אינסופית, פשוט כהרחבה פרידה ונורמלית:

הגדרה 2.1 הרחבה L/K אלגברית (לאו דווקא סופית) תיקרא:

1. פרידה/ספרבילית אם $L = \prod L_i$ כאשר L_i/K פרידות סופיות.

2. נורמלית אם $L = \prod L_i$ כאשר L_i/K נורמליות סופיות.

3. גלואה אם היא נורמלית ופרידה.

נגדיר עבור L/K את

$$\text{Gal}(L/K) = \text{Aut}_K(L) = \{\sigma : L \rightarrow L \mid \sigma|_K = \text{Id}, \sigma(x+y) = \sigma(x) + \sigma(y), \sigma(xy) = \sigma(x)\sigma(y)\}$$

חבורת גלואה.

שאלה האם יש התאמה $1-1$ בין תתי הרחבות של L/K ובין תתי חבורות של $\text{Gal}(L/K)$?

תשובה לא!

דוגמא ניקח את $\mathbb{Q}(\sqrt{p} \mid p \text{ is prime})$, הרחבה גלואה ואינסופית. אזי

$$\text{Gal}(L/\mathbb{Q}) \leq (\mathbb{Z}/2\mathbb{Z})^{\aleph_0}$$

ולמעשה יש אפילו איזומורפיזם (נוכיח תיכף). אם כן,

$$\text{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^{\aleph_0}$$

כאשר אם $\sigma = (\sigma_i)_{i=1}^{\infty}$, והראשונים מנויים $\{p_i\}_{i=1}^{\infty}$, אזי $\sigma(\sqrt{p_i}) = (-1)^{\sigma_i} \sqrt{p_i}$. כמות תתי החבורות היא יותר מאשר כמות תת הקבוצות של בסיס, שהיא לפחות $2^{\aleph_0}$ - אבל כמות ההרחבות של $\mathbb{Q}$ שיש בעולם היא לכל היותר $2^{\aleph_0}$, שכן כל הרחבה כזו היא תת קבוצה של מספרים אלגבריים, שמהם יש $\aleph_0$. משיקולי ספירה לא יכולה להיות התאמה כזו. נחזור להראות מה היא חבורת גלואה.

טענה 2.2 אם $p \nmid p_1, \dots, p_n$ ראשוניים כולם, אזי $\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ מופרדים לינארית ולכן $\text{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q})$.

הוכחה: די להראות כי $\sqrt{p} \notin \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$. נוכיח באינדוקציה על n . נניח שכולם שונים, ואז מההנחה:

$$\text{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q}) \cong \prod \text{Gal}(\mathbb{Q}(\sqrt{p_i})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$$

לכן תתי שדות של L מאינדקס 2 מעל $\mathbb{Q}$ מתאימים לתת חבורות מאינדקס 2 של $(\mathbb{Z}/2\mathbb{Z})^n$, ואלה מתאימות לתת קבוצות $\emptyset \neq S \subseteq \{1, \dots, n\}$ על ידי $\sqrt{\prod_{i \in S} p_i}$. ברור שהאיבר $\sqrt{p}$ לא בהרחבה של האיבר הזה, כי אחרת $p \cdot \prod_{i \in S} p_i \in \mathbb{Z}$ בסתירה. ■

כעת, נרצה להראות שעבור $L = \mathbb{Q}(\sqrt{p_i} \mid i = 1, 2, \dots)$ נקבל

$$\text{Gal}(L/\mathbb{Q}) = \prod_{i=1}^{\infty} \text{Gal}(\sqrt{p_i}/\mathbb{Q})$$

אם נגדיר $L_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$, ראינו שמתקיים

$$\text{Gal}(L/\mathbb{Q}) = \prod_{i=1}^n \text{Gal}(\sqrt{p_i}/\mathbb{Q})$$

כעת, יהי $(\varepsilon_i)_{i=1}^\infty$ ווקטור כלשהו של $\text{Gal}(\mathbb{Q}(\sqrt{p_i})/\mathbb{Q})$. נגדיר $\sigma_n \in \text{Gal}(L_n/\mathbb{Q})$. נגדיר $\varepsilon_i \in \text{Gal}(\mathbb{Q}(\sqrt{p_i})/\mathbb{Q})$. נגדיר, אם כן, $\sigma : L \rightarrow L$ על ידי $\sigma(x) = \sigma_n(x)$, אם $x \in L_n$. להיות $(\varepsilon_i)_{i=1}^n$. נגדיר, אם כן, $\sigma : L \rightarrow L$ על ידי $\sigma(x) = \sigma_n(x)$, אם $x \in L_n$.
 התחום הוא באמת L כי $L = \bigcup L_n$, וההגדרה היא טובה, כי אם $x \in L_n \cap L_m$, אזי $n \leq m$, אזי שתייהן לוקחות את הקואורדינטה n מתוך σ ומפעילות אותה על x .
 כלומר זה עובד באותה צורה. כעת, אם $x, y \in L$ אז יש m עם $x, y \in L_m$, ולכן $\sigma(x+y) = \sigma_m(x+y) = \sigma_m(x) + \sigma_m(y) = \sigma(x) + \sigma(y)$.
 וההופכי של σ הוא $\sigma^{-1}(x) = \sigma_n^{-1}(x)$, עבור $x \in L_n$. קיבלנו איזומורפיזם כמו שרצינו.

בתחילת המאה העשרים, קרול הגדיר טופולוגיה על $\text{Gal}(L/K)$, והוכיח את התאמת גלואה - התאמה $1-1$ בין תתי שדות לתתי חבורות סגורות.