

אלגברה ב2

© ארזים

17 במאי 2017

1 משפט גלואה

אנחנו רוצים להוכיח את משפט גלואה, שבכלליות אומר שלפולינום באיפיון 0 יש נוסחת שורשים אם ורק אם חבורת גלואה שלו פתירה. זה לא עובד באיפיון חיובי - למשל, $f(x) = x^p - x + \alpha$ אי פריק, אזי $\text{Gal}(f) = \mathbb{Z}/p\mathbb{Z}$, אבל אין נוסחת שורשים (דורש הוכחה). לפולינומים כאלה קוראים פולינומי ארטיין-שרייר, והם התחליף של $x^p - \alpha$ שאינם פרידים. אז משפט גלואה הוא נכון אם מחליפים נוסחת שורשים בנוסחת שורשים ועוד ארטיין-שרייר, ואת חבורת גלואה בחבורת האוטומורפיזמים.

1.1 הרחבות מעגליות

טענה 1.1 אם K שדה מאיפיון $p \geq 0$ ואם $p \nmid n$, אזי יש שורש יחידה פרימיטיבי מסדר n , שנסמנו ζ_n . הכוונה - $\zeta_n^n = 1$, וכן $\zeta_n^k \neq 1$ לכל $k < n$.

הוכחה: נסתכל על השורשים של $x^n - 1$. יש n כאלו כי $\gcd(x^n - 1, nx^{n-1}) = 1$. אלה מהווים חבורה ביחס לכפל: אם $\alpha^n = 1, \beta^n = 1$ אזי

$$(\alpha\beta)^n = \alpha^n \beta^n = 1$$

קעת, אם נסמן μ_n את אוסף השורשים, אז $\mu_n \subseteq \overline{K}^*$ סופית - כלומר היא ציקלית, ולכן יש לה יוצר, שהוא שורש פרימיטיבי. ■

הערה 1.2 באיפיון p אי שורש יחידה פרימיטיבי מסדר p כי $x^p - 1 = (x - 1)^p$. עם זאת, שורשי $f(x) = x^p - x$ הם חבורה: $(\mathbb{F}_p, +)$.

משפט 1.3 נניח כי K שדה עם שורש יחידה פרימיטיבי מסדר n בתוך K (בפרט $\text{char} K \nmid n$). כלומר $\mu_n \subseteq K$. נניח גם שיש L/K , עם $\alpha \in L$, $L = K(\alpha)$ וגם $\alpha^n = a \in K$. אזי L/K גלואה, וכן

$$\text{Gal}(L/K) = C_d$$

באשר C_d ציקלית מסדר n | d . יתר על כן, אם $\alpha^d \notin K$ לכל $d < n$, עם $d < n$, אז $\text{Gal}(L/K) \cong C_n$.

הוכחה: כיוון שמתקיים $\alpha^n = a$, לכל σ שיכון של K מעל K (לסגור אלגברי) מתקיים $(\sigma(\alpha))^n = a$, מצד שני.

$$x^n - a = \prod_{\xi \in \mu_n} (x - \xi a)$$

לכן, אם $\alpha \neq 0$ (ואפשר להניח זאת) אז יש בתוך L בדיוק n שורשים שהם $\{\xi a \mid \xi \in \mu_n\}$ לכן L/K גלואה. ההעתקה

$$\begin{aligned} \varphi : \text{Gal}(L/K) &\rightarrow \mu_n \cong C_n \\ \varphi(\sigma) &= \frac{\sigma(\alpha)}{\alpha} \in \mu_n \end{aligned}$$

היא מונומורפיזם, כי אם $\sigma(\alpha) = \alpha$ אזי $\sigma = \text{id}$. לכן

$$\text{Gal}(L/K) \cong H \leq C_n$$

זוה מוכיח את החלק הראשון, כי $d \mid n, H \cong C_d$. אם φ לא על, ואם σ יוצר של $\text{Gal}(L/K)$, אזי $\sigma^d = 1$ עבור $d \mid n, d < n$. אז $\sigma(\alpha) = \eta \alpha$, באשר η שורש יחידה פרימיטיבי מסדר d . אזי

$$\text{irr}(\alpha, K) = \prod_{i=0}^{d-1} (x - \sigma^i(\alpha)) = \prod_{i=0}^{d-1} (x - \eta^i \alpha) = x^d - \alpha^d \in K[x]$$

על כן $\alpha^d \in K$, עבור $d \mid n, d < n$, כנדרש. ■

משפט 1.4 נניח כי $\mu_n \subseteq K$. תהי L/K הרחבת גלואה כך שמתקיים $C_n \cong \text{Gal}(L/K)$. אזי יש $\alpha \in L$ כך שמתקיים $L = K(\alpha), \alpha^n = a \in K$.

הוכחה: נקח $\sigma \in \text{Gal}(L/K)$ מסדר n . נחפש איבר שצמודיו יהיו $\{\xi a \mid \xi \in \mu_n\}$, כי אז α ממעלה n ולכן יוצר את L/K וכמובן $\alpha^n = a \in K$. $\text{irr}(\alpha, K) = x^n - a \in K[x]$. די למצוא α כך שמתקיים $\sigma(\alpha) = \zeta \alpha$, באשר ζ שורש יחידה פרימיטיבי. ניקח α מהצורה:

$$\alpha = \sum_{i=0}^{n-1} \zeta^{-i} \sigma^i(\beta) = \sum_{i=1}^n \zeta^{-i} \sigma^i(\beta)$$

כי אז

$$\sigma(\alpha) = \sum_{i=0}^{n-1} \zeta^{-i} \sigma^{i+1}(\beta) = \sum_{i=1}^n \zeta^{-i+1} \sigma^i(\beta) = \zeta^{-1} \alpha$$

די למצוא כזה β , עבורו $\alpha \neq 0$. זה נכון כי מאי תלות של קרקטרים ההעתקה

$$\sum_{i=0}^{n-1} \zeta^{-i} \sigma^i$$

■ אינה טריוויאלית, ולכן יש $\beta \in L$ שתמונתו, שהיא α , אינה 0.

הגדרה 1.5 נאמר כי L/K היא מעגלית אם היא גלואה וחבורת גלואה שלה מעגלית.

משפט 1.6 נניח שבתוך K יש שורש יחידה פרימיטיבי מסדר n . אזי יש התאמה חד-חד-ערכית ועל בין הרחבות מעגליות מסדר n של K (בתוך סגור אלגברי) לבין תתי חבורות ציקליות של K^*/K^{*n} , כאשר $K^{*n} = \{x^n \mid x \in K^*\}$ (זהו חלק מהמשפט היסודי של תורת קומר).

הוכחה: בהנתן L/K מעגלית מסדר n , ראינו שמתקיים $L = K(\sqrt[n]{a})$, כאשר $a \in K^*$. נתאים את L לחבורה שנוצרת על ידי a בתוך K^*/K^{*n} . צריך להראות שזה מוגדר היטב, חד-חד-ערכי ועל.

זה שזה על נובע מהמשפט הראשון שהוכחנו היום, כי אם $H \leq K^*/K^{*n}$ מסדר n ציקלית, אזי $H = \langle aK^{*n} \rangle$. לכן לכל $d \mid n$ עם $d < n$ מתקיים $a^d \notin K^{*n}$, כלומר $\sqrt[n]{a^d} \notin K$. לכן

$$C_n \cong \text{Gal}(K(\sqrt[n]{a})/K)$$

נוכיח חד-חד-ערכיות. נניח כי $a, b \in K^*$ יוצרים את אותה חבורה מסדר n בתוך K^*/K^{*n} . אזי מתקיים

$$aK^{*n} = b^i K^{*n}$$

כאשר i, n זרים. לכן $a = b^i c^n$, עבור $c \in K^*$ כלשהו. לכן נקבל כי

$$K(\sqrt[n]{a}) = K(\sqrt[n]{b^i}) \subseteq K(\sqrt[n]{b})$$

מסימטריה יש שוויון.

נותר להראות שההתאמה מוגדרת היטב - נקח $a, b \in K^*$ עבורם

$$L = K(\sqrt[n]{b}) = K(\sqrt[n]{a})$$

נרצה לראות כי $\langle aK^* \rangle = \langle bK^* \rangle$. נסמן $\alpha = \sqrt[n]{a}$, $\beta = \sqrt[n]{b}$. אזי $1, \alpha, \dots, \alpha^{n-1}$ בסיס של L/K , ונכתוב

$$\beta = \sum_{j=0}^{n-1} c_j \alpha^j$$

עבור σ שיוצר את חבורת גלואה של ההרחבה, $\sigma(\alpha) = \zeta\alpha$ כאשר ζ שורש יחידה פרימיטיבי מסדר n . כמו כן, $\sigma(\beta) = \zeta'\beta$ כאשר ζ' שורש יחידה פרימיטיבי מסדר n . לכן $\zeta' = \zeta^i$ כאשר i, n זרים. נפעיל את σ על השוויון האחרון שראינו, ואז

$$\sigma(\beta) = \zeta'\beta = \sum_{j=0}^{n-1} c_j \zeta' \alpha^j$$

$$\sigma(\beta) = \sum_{j=0}^{n-1} c_j \zeta^j \alpha^j$$

מהשוואת מקדמים נקבל

$$\zeta' c_j = \zeta^j c_j$$

מכאן, לכל j עם $c_j \neq 0$, מתקיים $\zeta' = \zeta^j$. נובע שיש j יחיד כזה, ומפרימיטיביות j, n זרים. נקבל

$$\beta = c_i \alpha^i$$

ולכן

$$b = c_i^n \alpha^i$$

ולכן

$$\langle aK^{*n} \rangle = \langle bK^{*n} \rangle$$

■

תרגיל

1. אם $\text{char}K = p > 0$ וכן $a \in K$, אם נסמן בתור α שורש של $f(x) = x^p - x - a$ אזי שורשי f הם

$$\{\alpha, \alpha + 1, \dots, \alpha + p - 1\} = \alpha + \mathbb{F}_p$$

2. הסיקו כי $K^{(\alpha)}/K$ גלואה מסדר p או 1.

3. נסמן $p(x) = x^p + x$ אזי $p : (K, +) \rightarrow (K, +)$ הומומורפיזם.

4. יש התאמה חד-חד-ערכית ועל בין L/K מעגליות מסדר p לבין תתי חבורות של $(K, +)/(p(K), +)$.