

אלגברה ב2

© ארזים

9 במאי 2017

טענה 0.1 יהי $n \in \mathbb{N}$ ויהי F שדה שבו $0 \neq n$. אזי

$$\left| \left\{ \lambda \in \overline{F}^* \mid \lambda^n = 1 \right\} \right| = n$$

וכן יש שורש יחידה פרימיטיבי מסדר n .

הוכחה: הקבוצה הזו היא קבוצת שורשי $x^n - 1$ בתוך $\overline{F}$. כדי להראות שגודלה הוא n מספיק להשתכנע שאין שורשים משותפים של $x^n - 1, (x^n - 1)'$. הנגזרת היא nx^{n-1} , והנחנו $n \neq 0$, ולכן השורש היחיד שלה הוא 0. לא מקיים $x^n - 1 = 0$, ועל כן אי שורשים משותפים. לכן יש n איברים.

הקבוצה הזו היא תת חבורה סופית של $\overline{F}^*$, ולכן היא ציקלית - כל יוצר שלה הוא שורש יחידה פרימיטיבי מסדר n . ■

טענה 0.2 בסימוני הטענה הקודמת, יהי $\zeta_n \in \overline{F}$ שורש יחידה פרימיטיבי מסדר n . ההרחבה $F(\zeta_n)/F$ הינה גלואה, והחבורה המתאימה $\text{Gal}(F(\zeta_n)/F)$ ניתנת לשיכון בתוך $(\mathbb{Z}/n\mathbb{Z})^*$.

הוכחה: ζ_n מקיים את $x^n - 1$ ולכן ההרבה היא אלגברית. נסמן $f = \text{irr}(\zeta_n, F)$, ואז $f \mid x^n - 1$, ולכן f פריד - כי כל שורשי $x^n - 1$ שונים זה מזה. לכן $F(\zeta_n)/F$ פרידה. כמו כן, ההרחבה נורמלית, כי כל השורשים של f הם שורשי יחידה מסדר n , ולכן חזקות של ζ_n . לכן ההרחבה היא גלואה. נראה את השיכון. יהי $\sigma \in \text{Gal}(F(\zeta_n)/F)$. מתקיים

$$\sigma(\zeta_n) = \zeta_n^{k(\sigma)}$$

כאשר $\gcd(n, k(\sigma)) = 1$. נשים לב כי $k : \text{Gal}(F(\zeta_n)/F) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ היא הומומורפיזם של חבורות:

$$\zeta_n^{k(\sigma\tau)} = (\sigma\tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{k(\tau)}) = \left(\zeta_n^{k(\tau)}\right)^{k(\sigma)} = \zeta_n^{k(\sigma)k(\tau)}$$

החד-חד-ערכיות ברורה - כל σ מוגדר באופן יחיד על ידי הפעולה שלו על ζ_n , שיוצר את ההרחבה, ולכן מוגדר באופן יחיד על ידי הערך $k(\sigma)$. ■

דוגמה כאשר $F = \mathbb{C}$ התמונה של k היא $\{1\}$ - חבורת גלואה טריוויאלית. כאשר $n = p$, $F = \mathbb{Q}$, ראשוני, הפולינום $x^{p-1} + \dots + x + 1$ אי פריק, ולכן ההרחבה $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ היא ממעלה $p - 1 = |(\mathbb{Z}/p\mathbb{Z})^*|$. נובע כי ההעתקה k היא על.

תזכורת

$$|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$$

הגדרה 0.3 ניקח $F = \mathbb{Q}$. נגדיר את הפולינום הציקלוטומי מסדר n :

$$\mathbb{Z}[x] \ni \Phi_n(x) = \frac{x^n - 1}{\text{lcm}_{n \neq d|n} (x^d - 1)} = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (x - \zeta_n^k)$$

משפט 0.4 זהו פולינום אי פריק מעל $\mathbb{Q}$.

הוכחה: נניח בשלילה שיש פירוק לא טריוויאלי:

$$\Phi_n(x) = f(x)g(x)$$

ראשית, נניח כי לכל שורש ζ של f , ולכל ראשוני p שלא מחלק את n , ζ^p שורש של f .
יהי ζ שורש של f , ויהי ζ^m שורש של $\Phi_n(x)$. בפירוק של m לראשוניים (לא בהכרח שונים),
 $m = p_1 \cdots p_l$, מתקיים $p_i \nmid n$ לכל i - כי אחרת n, m לא זרים, אבל הם כן. אם כן,

$$\zeta^m = \left(((\zeta^{p_1})^{p_2})^{\cdots} \right)^{p_l}$$

באינדוקציה נובע כי ζ^m הוא שורש של f ולכן $f(x) = c\Phi_n(x)$, וזאת סתירה לקיום הפירוק.

לכן, נובע שקיימים שורש ζ של f וראשוני p שלא מחלק את n עבורם ζ^p אינו שורש של f . ζ^p הוא כן שורש של $\Phi_n(x)$, ולכן נובע שהוא שורש של g . לכן,

$$\gcd(f(x), g(x^p)) \neq 1$$

ותכונה זו נשמרת לאחר רדוקציה מודולו p - כלומר יש להם מחלק משותף לא טריוויאלי מתוך $\mathbb{F}_p[x]$. נובע כי בתוך $\overline{\mathbb{F}_p}$, יש לפולינום $\Phi_n(x) = f(x)g(x)$ - כי $x^p = x$ מעל $\mathbb{F}_p$ לכל x , כלומר השורשים של g ושל $g(x^p)$ הם אותם שורשים. לכן, לפולינום $x^n - 1$ יש שורש כפול בתוך $\overline{\mathbb{F}_p}$ - בסתירה לכך שמתקיים $p \nmid n$. לכן סתרנו את קיום הפירוק. ■

מסקנה 0.5 מתקיים $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

הוכחה: $\Phi_n(\zeta_n) = 0$ ולכן $\Phi_n(x) = \text{irr}(\zeta_n, \mathbb{Q})$. לכן $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n(x)$. המעלה הזו היא הסדר של חבורת גלואה של ההרחבה, ולכן ההומומורפיזם $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ שהגדרנו הוא מומומורפיזם בין חבורות מאותו סדר - כלומר איזומורפיזם. ■