אלגברה ב2

ⓒ ארזים

9 במאי 2017

טענה 0.1 יהי $n \in \mathbb{N}$ ויהי F שדה שבו $n \neq 0$. 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. 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 $\mathrm{Gal}\left(F(\zeta_n)/F\right)$ ניתנת לשיכון בתוך $(\mathbb{Z}/n\mathbb{Z})^*$.

הוכחה: ζ_n מקיים את $x^n - 1$ ולכן ההרבה היא אלגברית. נסמן $f = \mathrm{irr}(\zeta_n, F)$, 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 $\sigma \in \mathrm{Gal}\left(F(\zeta_n)/F\right)$. מתקיים

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

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

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

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 $k(\sigma)$. ■

דוגמא כאשר $F = \mathbb{C}$ התמונה של k היא $\{1\}$ - חבורת גלואה טריוויאלית.

כאשר $F = \mathbb{Q}$, $n = p$ ראשוני, הפולינום $x^{p-1} + \cdots + x + 1$ אי פריק, ולכן ההרחבה $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ היא ממעלה $\left|(\mathbb{Z}/p\mathbb{Z})^*\right| = p - 1$. נובע כי ההעתקה k היא על.

תזכורת

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

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

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

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

הוכחה: נניח בשלילה שיש פירוק לא טריוויאלי:

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

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 $\Phi_n\left(x\right)$. 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,

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

באינדוקציה נובע כי ζ^m הוא שורש של f ולכן $f\left(x\right) = c\Phi_n\left(x\right)$, 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 $\Phi_n\left(x\right)$, ולכן נובע שהוא שורש של g. לכן,

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

ותכונה זו נשמרת לאחר רדוקציה מודולו p - כלומר יש להם מחלק משותף לא טריוויאלי מתוך $\mathbb{F}_p\left[x\right]$. נובע כי בתוך $\overline{\mathbb{F}_p}$, יש לפולינום $\Phi_n\left(x\right) = f\left(x\right)g\left(x\right)$ - כי $x^p = x$ מעל $\mathbb{F}_p$ לכל x, כלומר השורשים של g ושל $g\left(x^p\right)$ 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 $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^*$, $\left[\mathbb{Q}\left(\zeta_n\right) : \mathbb{Q}\right] = \phi\left(n\right)$.

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