אלגברה ב' 2 – הרצאה 19

4.5.11

שורשי יחידה

ניקח שדה K, $\tilde{K}$ הסגור האלגברי שלו. K^* חבורה ביחס לכפל, $n \in \mathbb{N}$

הגדרה. איבר $\zeta \in K^*$ נקרא:

1. שורש יחידה n–י אם $\zeta^n = 1$, כלומר $\operatorname{ord}\zeta | n$. קבוצת כל שורשי היחידה ה– n–ים מסומן $\mu_n(K)$.
2. שורש יחידה n–י נקרא פרימיטיבי אם $\zeta^n = 1$, $\zeta^k \neq 1$ לכל $1 \leq k \leq n$. כלומר $\operatorname{ord}\zeta = n$.
3. שורש יחידה אם יש $n \in \mathbb{N}$ כך ש– $\zeta^n = 1$. קבוצת שורשי היחידה ב– K תסומן $\mu(K)$. כלומר, $\operatorname{ord}\zeta < \infty$.

הערות.

1. $\mu_n(K)$ היא קבוצת השורשים של $x^n - 1$ ב– K. לכן, $|\mu_n(K)| \leq n$.
2. $|\mu_n(\tilde{K})| = n \Leftrightarrow$ כאשר $x^n - 1$ פריד $\Leftrightarrow \operatorname{chr} K \nmid n$.
3. $\mu_n(K)$ היא תת חבורה של K^*; היא סופית, לכן (ממשפט) מעגלית.
4. אם $\zeta \in \mu_n(K)$ פרימיטיבי אז $\langle\zeta\rangle = \mu_n(K)$ ו– $|\mu_n(K)| = n$.
5. $\zeta \in \mu_n(\tilde{K})$ פרימיטיבי $\Leftrightarrow \operatorname{chr} K \nmid n$.

למה. נסמן, $W = \mu_n(\tilde{K})$. יהי $\zeta \in W$ פרימיטיבי. אז $K(\zeta) = K(W)$ הרחבת גלואה סופית של K ויש שיכון של חבורות $i : \operatorname{Gal}(K(\zeta)/K) \to (\mathbb{Z}/n\mathbb{Z})^*$, הנתון ע"י $\zeta^{i(\sigma)} = \sigma(\zeta)$.

הוכחה. $W \ni \zeta$ לכן $K(\zeta) \subseteq K(W)$. להפך, כל $\xi \in W$ הוא חזקה של ζ לכן $\xi \in K(\zeta)$. לכן, $W \subseteq K(\zeta)$ ולכן $K(W) \subseteq K(\zeta)$. קיבלנו $K(W) = K(\zeta)$.
W היא קבוצת השורשים של הפולינום $x^n - 1$ לכן $K(W)$ הוא שדה הפיצול של הפולינום הזה ולכן זאת הרחבה נורמלית של K. כמו כן, $x^n - 1$ פריד, לכן $K(W)/K$ פרידה ולכן גלואה.
יהי $\sigma \in \operatorname{Gal}(K(W)/K)$ אז $(\sigma(\zeta))^n = \sigma(\zeta^n) = \sigma(1) = 1$ לכן $\sigma(\zeta) \in W$. לכן, קיים $i \in \mathbb{Z}$ כך ש– $\sigma(\zeta) = \zeta^i$. i כזה לא בהכרח יחיד, אבל $\zeta^i = \zeta^j \Leftrightarrow \zeta^{i-j=1} \Leftrightarrow n = (i-j)|\operatorname{ord}\zeta$. כלומר i לא יחיד, אבל יחיד מודולו n. לכן, התמונה של $i \in \mathbb{Z}$ ב– $\mathbb{Z}/n\mathbb{Z}$ היא יחידה. נסמן אותה $i(\sigma)$. בכך הגדרנו העתקה $i : \operatorname{Gal}(K(W)/K) \to \mathbb{Z}/n\mathbb{Z}$ שמקיימת $\zeta^{i(\sigma)} = \sigma(\zeta)$.
ברור ש– $i(1) = 1$.

אם $\sigma, \tau \in \mathrm{Gal}(K(W)/K)$ אז

$$\zeta^{i(\sigma\tau} = \sigma\tau(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{i(\tau)}) = (\sigma(\zeta))^{i(\tau)} = \zeta^{i(\sigma)i(\tau)}$$

לכן, $i(\sigma\tau) = i(\sigma)i(\tau)$.
בפרט, $1 = i(1) = i(\sigma)i(\sigma^{-1})$, לכן $i(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$ לכן זה הומומורפיזם של חבורות.
i חח"ע: יהי $\sigma \in \ker i$, אז $\zeta = \zeta^1 = \zeta^{i(\sigma)} = \sigma(\zeta)$. אז σ משבית כל איבר ב- $K(\zeta)$ לכן $\sigma = 1$. □

הערות.

1. $(\mathbb{Z}/n\mathbb{Z})^* = \{k + n\mathbb{Z} : 0 \le k < n,\ k, n \text{ זרים}\}$. ואכן, $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ הפיך
$\Leftrightarrow$ יש $m \in \mathbb{Z}$ כך ש- $km \equiv 1 (\mod n)$
$\Leftrightarrow$ יש $l, m \in \mathbb{Z}$ כך ש- $km - 1 = nl$
$\Leftrightarrow$ יש $l, m \in \mathbb{Z}$ כך ש- $km + nl = 1$ זרים.
לכן, $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n) := |\{K : 0 \le k < n,\ k, n \text{ זרים}\}|$ פונקציית אוילר.

2. משפט השאריות הסיני: אם $m, n \in \mathbb{N}$ זרים אז יש איזומורפיזם של חוגים:
$a + mn\mathbb{Z} \to (a + m\mathbb{Z}, a + n\mathbb{Z})$ ע"י $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. לכן,
$(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. בפרט, $\varphi(mn) = \varphi(m)\varphi(n)$.
בפרט, $(\mathbb{Z}/p_1^{m_1} \dots p_n^{m_n}\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{m_1}\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_n^{m_n}\mathbb{Z})^*$ כאשר
$p_1, \dots, p_n$ ראשוניים שונים. לכן, $\varphi(p_1^{m_1} \dots p_n^{m_n}) = \varphi(p_1^{m_1}) \dots \varphi(p_n^{m_n})$.

3. יהי p ראשוני $\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$. ביתר דיוק אם $p \ne 2$ אז
$(\mathbb{Z}/p^m\mathbb{Z})^* = \mathbb{Z}/p^{m-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{Z}/p^{m-1}(p-1)\mathbb{Z}$
ואם $(\mathbb{Z}/2^m\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$
ללא הוכחה. רק כדי שנוכל להשתמש בהמשך.

מסקנה. יהי $\zeta \in \tilde{K}$ שורש יחידה n-י פרימיטיבי. $[K(\zeta) : K] \le \varphi(n)$ ו- $\mathrm{Gal}(K(\zeta)/K)$ אבלית.

משפט. יהי $\zeta \in \tilde{Q}$ שורש יחידה n-י פרימיטיבי.

1. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.
2. $\mathrm{Gal}(\mathbb{Q}(r)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

הוכחה. נראה תחילה ששני הסעיפים במשפט שקולים. ואכן, אנו יודעים כי $\mathrm{Gal}(\mathbb{Q}(r)/\mathbb{Q})$ איזומורפי לתת חבורה של $(\mathbb{Z}/n\mathbb{Z})^*$ וכן $\varphi(n) = |(Z/n\mathbb{Z})^*|$.
לכן נוכיח את הסעיף הראשון. יהי $f = \mathrm{irr}(\zeta, \mathbb{Q})$ אזי $\deg(f) \le \varphi(n)$. לכן, די להראות ש- $\deg f \ge \varphi(n)$.
לשם כך, מספיק להראות כי כל שורש יחידה n-י הוא שורש של f (כי יש בדיוק $\varphi(n)$ שורשים פרימיטיביים, כי יש בדיוק $\varphi(n)$ יוצרים לתמורה ציקלית מסדר n). כל שורש כזה הוא מהצורה ζ^k כאשר k זר ל- n. לכן די להראות כי $f(\zeta^k) = 0$ לכל k זר ל- n.
נראה כי אם $f(\xi) = 0$ אז $f(\xi^k) = 0$ לכל j זר ל- n. כמו כן, אנו יודעים $k = p_1, \dots p_m$ כאשר p_i ראשוני לכל i, זר ל- n.
באינדוקציה, כל מה שעלינו להוכיח הוא שאם $f(\xi) = 0$ אז $f(\xi^p) = 0$ לכל p ראשוני המקיים $p \nmid n$. נוכיח זאת. $f|x^n - 1$, לכן $x^n - 1 = fh$ עבור איזשהו $h \in \mathbb{Q}[x]$, f, h מתקונים. לפי הלמה של גאוס $f, h \in \mathbb{Z}[x]$. כעת, $(\xi^p)^n = (\xi^n)^p = 1^p = 1$, לכן ξ^p שורש של fh.
נניח בשלילה כי ξ^p שורש של h. כלומר $h(\xi^p) = 0$ לכן ξ שורש של $h(x^p)$. לכן $f|h(x^p)$, לכן קיים $g \in \mathbb{Q}[x]$ כך ש- $h(x^p) = fg$. $f, h(x^p)$ מתוקנים, לכן g מתוקן ולכן עפ"י הלמה

של גאוס $g \in \mathbb{Z}[x]$. עבור $a \in \mathbb{Z}$ נסמן $\tilde{a}$ את התמונה של a ב- $F_p = \mathbb{Z}/p\mathbb{Z}$ ועבור כל $q = \sum b_i x^i \in \mathbb{Z}[x]$ נסמן $\tilde{q} = \sum \tilde{b}_i x^i \in F_p[x]$.
אם $h = \sum_{i=0}^{\infty} a_i x^i \in \mathbb{Z}[x]$ אז

$$\tilde{f} \cdot \tilde{g} = \widetilde{f \cdot g} = \widetilde{h(x^p)} = \sum_{i=0}^{\infty} \tilde{a}_i^p (x^i)^p = \sum_{i=0}^{\infty} (\tilde{a}_i x^i)^p = (\sum_{i=0}^{\infty} \tilde{a}_i x^i)^p = \tilde{h}^p$$

מכאן כל שורש של $\tilde{f}$ הוא שורש של $\tilde{h}$. אולם, אנחנו יודעים כי $x^n - 1 = f \cdot h$ ולכן $x^n - 1 = \tilde{f} \cdot \tilde{h}$. לכן כל שורש של $\tilde{f}$ הוא שורש מרובה של $x^n - 1$ (כפולינום מעל F_p), וזאת סתירה כי $x^n - 1 \in F_p[x]$ פריד כי $(x^n - 1)' = n(x^{n-1})$ וכן $p \nmid n$, ולכן אין שורשים משותפים ל- $x^n - 1$ ול- $(x^n - 1)'$. לכן t^p שורש של f, כפי שרצינו.
נחזור להוכחה של המשפט. לכן לכל k זר ל- n, $f(\zeta^k) = 0$ ולכן יש לפחות $\varphi(n)$ שורשים, לכן $\deg f \geq \varphi(n)$ ובסה"כ $\deg(f) = \varphi(n)$ וכן $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. □

נסמן ב- $\zeta_n \in \widetilde{\mathbb{Q}}$ שורש יחידה n-י פרימיטיבי (נבחר כלשהו) ונסמן $f_n = \mathrm{irr}(\zeta_n, \mathbb{Q})$.

מסקנות.

1. $$f_n(x) = \prod_{\zeta \text{ שורש פרימיטיבי (יחידה ה-}n\text{-י)}} (x - \zeta) = \prod_{\substack{k \text{ זר ל-}n \\ 0 \leq k < n}} (x - \zeta_n^k)$$

2. $$x^n - 1 = \prod_{\zeta \text{ שורש פרימיטיבי (יחידה ה-}n\text{-י)}} (x - \zeta) = \prod_{k=0}^{n-1} (x - r_n^k) = \prod_{d|n} f_d(x)$$

   את השוויון האחרון לא נוכיח היום.
   לכן, $f_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} f_d(x)}$.

3. $f_1(x) = x + 1$ ולכן:

$$f_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

עבור p ראשוני.

מסקנות. (מהמסקנות)
אם m, n זרים אז:

1. $Q(\zeta_{mn}) = \mathbb{Q}(\zeta_n) \cdot \mathbb{Q}(\zeta_m)$.
2. $\mathbb{Q} = \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$.

הוכחה.

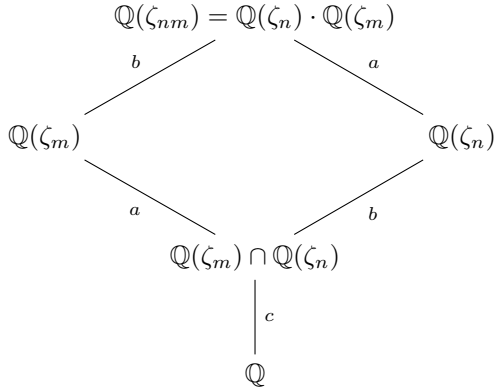
1. נוכיח הכלה דו כיוונית.

$\subseteq$: $\mathrm{ord}(\zeta_n)=n$, $\mathrm{ord}(\zeta_m)=m$ ולכן $\mathrm{ord}(\zeta_n\zeta_m)=n\cdot m$. לכן $\zeta_n\zeta_m$ שורש יחידה $n\cdot m$–י פרימיטיבי, ולכן ζ_{mn} חזקה שלו, ובפרט:

$$\mathbb{Q}(\zeta_{mn})\subseteq\mathbb{Q}(\zeta_m\zeta_n)\subseteq\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$$

$\supseteq$: $\mathrm{ord}(\zeta_{mn}^n)=m$, כלומר ζ_{mn}^n שורש יחידה m–י פרימיטיבי. לכן ζ_m חזקה שלו, לכן $\mathbb{Q}(\zeta_{mn})\subseteq\mathbb{Q}(\zeta_{mn}^n)\subseteq\mathbb{Q}(\zeta_m)$. באופן דומה $\mathbb{Q}(\zeta_{mn})\subseteq\mathbb{Q}(\zeta_n)$ ולכן $\mathbb{Q}(\zeta_n)\cdot\mathbb{Q}(\zeta_m)\subseteq\mathbb{Q}(r_{mn})$.

2.



מהתרשים נקבל:

$\varphi(mn)=abc$, $\varphi(m)=ac$, $\varphi(n)=bc$, אולם $\varphi(mn)=\varphi(m)\varphi(n)$ לכן $abc=acbc$ לכן $c=1$. כלומר $\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\zeta_m)=\mathbb{Q}$.

□