אלגברה ב' 2 – הרצאה 16

11.4.11

אנחנו רוצים לסיים להוכיח את המשפט משבוע שעבר. ראינו שכל איבר $z \in \mathbb{C}$ הוא ריבוע.

טענה. ל- $\mathbb{C}$ אין הרחבה ריבועית.

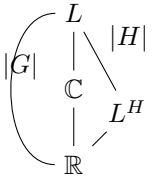
הוכחה. תהי $L/\mathbb{C}$ ממעלה 2. אז $L = \mathbb{C}(\alpha)$ כאשר α הוא שורש של $f = x^2 + bx + c \in \mathbb{C}[x]$.
לכן,

$$0 = \alpha^2 + b\alpha + c = \left(\alpha + \frac{b}{2}\right)^2 + c - \left(\frac{b}{2}\right)^2$$

כלומר $(\alpha + b/2)^2 = (b/2)^2 - c$. לפי הטענה הקודמת, $\left(\frac{b}{2}\right)^2 - c \in \mathbb{C}^2$. לכן, $\alpha + \frac{b}{2} = \pm\sqrt{\left(\frac{b}{2}\right) - c} \in \mathbb{C}$ לכן גם $\alpha \in C$ וזאת סתירה לכך ש- L/C ממעלה 2. □

משפט. $\mathbb{C}$ סגור אלגברית.

הוכחה. תהי $C/\mathbb{C}$ הרחבה אלגברית. צ"ל $L = \mathbb{C}$. בה"כ נניח L/C סופית כי כל הרחבה אלגברית היא איחוד של סופיות, לכן אם כולן $\mathbb{C}$ גם האיחוד הוא $\mathbb{C}$.
$L/\mathbb{C}$ הרחבה פרידה (כי $\operatorname{char}\mathbb{C} = 0$). לכן, $L/\mathbb{R}$ סופית, פרדיה. בה"כ $L/\mathbb{R}$ גלואה, אחרת נחליף את L בסגור גלואה של L/R. נשתמש קצת בתורת החבורות. נסמן $G = \operatorname{Gal}(L/R)$ ותהי $H \leq G$ חבורה 2-סילו של G (מבחיתנו גם חבורה בת איבר אחד גודלה חזקה של 2). אז $|H|$ הוא חזקה של 2 והאינדקס $[G : H]$ הוא זר ל-2, כלומר איזוגי. יהיה L^H שדה השבת של H. אז $[L^H : \mathbb{R}] = \frac{|G|}{|H|} = (G : H)$ (מכלל המגדל) איזוגי.



יש $\alpha \in L^H$ כך ש- $L^H = \mathbb{R}(\alpha)$. יהי $f = \operatorname{irr}(\alpha, \mathbb{R})$ אז $\deg f$ איזוגי. לכן לפי ההנחה יש ל-f שורש ב- $\mathbb{R}$. אבל f אי פריק לכן $\deg f = 1$ ולכן $\alpha \in \mathbb{R}$. מכאן $L^H = \mathbb{R}$ לכן $H = G$ כלומר G חבורת 2.
לכן $G_1 := \operatorname{Gal}(L/\mathbb{C}) \leq G$ מאינדקס $[\mathbb{C} : \mathbb{R}] = 2$. גם G_1 חבורת 2 לכן אם $G_1 \neq 1$ יש לה תת-חבורה G_2 כך ש- $(G_1 : G_2) = 2$. אז $(L^{G_1} : \mathbb{C}) = 2$. סתירה לטענה הקודמת.
לכן $G_1 = 1$ וזה אומר $|G| = 2$. מתוך $\mathbb{R} \subseteq \mathbb{C} \subseteq L$ $[L : \mathbb{R}] = 2 = [\mathbb{C} : \mathbb{R}]$ לכן $L = \mathbb{C}$. □

הערה. $\text{char} = 0$ כי הנחנו שיש מספרים חיוביים, סכום של חיוביים חיובי ולכן $1 + 1 + \ldots + 1 > 0$

דוגמא. יהי K שדה, $t_1, \ldots, t_k$ משתנים בלתי תלוים מעליו. אז S_n פועלת על החוג $K[t_1, \ldots, t_n]$ (ע"י פעולה על $\{t_1, \ldots, t_n\}$. זה מגדיר פעולה על $L = K(t_1, \ldots, t_n)$ לכן $S_n \leq \text{Aut}(L)$. נסמן $E = L^{S_n}$ אז לפי הלמה של ארטין L/E גלואה סופית, $\text{Gal}(L/E) = S_n$. זה מוכיח שאפשר לראות את S_n כחבורת גלואה. לכן כל חבורה סופית היא חבורת גלואה: אם $G \leq S_n$ אז G היא חבורת גלואה $G = \text{Gal}(L/L^G)$.
מהו E? יהיו $S_1, \ldots, S_n$ הפולינומים הוסימטריים היסודיים ב- $t_1, \ldots, t_n$. אז $S_1, \ldots, S_n \in E$ כלומר $E_0 = K(S_1, \ldots, S_n) \subseteq E$.
$f(x) := (x - t_1) \ldots (x - t_n) = x^n - S_1 x^{n-1} + S_2 x^{n-2} + \ldots + (-1)^n S_n \in E_0[x]$.
ובוודאי $L = E_0(t_1, \ldots, t_n)$ ולכן $[L : E_0] \leq n!$. אבל $[L : E] = |S_n| = n!$ לכן $E = E_0$. קיים הומומורפיזם של חוגים $\omega : K[t_1, \ldots, t_n] \to_K L[S_1, \ldots, S_n]$ כך ש- $t_i \mapsto s_i$. הוא על. בקמרה שלנו הוא גם חח"ע: הגרעין הוא

$$\{g \in K[t_1, \ldots, t_n] | g(S_1, \ldots, S_n) = 0\} = \{0\}$$

לפי משפט.
לכן יש לנו איזומורפיזם ואז הוא ניתן להרחבה לשדות המנות. כלומר $K(t_1, \ldots, t_n) \to K(S_1, \ldots, S_n)$.

מסקנה. יהי K שדה ויהיו $t_1, \ldots, t_n$ משתנים מעל השדה הזה. יהי L שדה הפיצול של $g = x^n + t_1 x^{n-1} + \ldots + t_n \in K(t_1, \ldots, t_n) =: E$. אז L/E גלואה סופית ו- $\text{Gal}(L/E) \cong S_n$.

הוכחה. הוכחנו זאת עם הפולינום $f = x^n - t_1 x^{n-1} + \ldots + (-1)^n t_n$ במקום g (אפילו הוכחנו ל- s במקום t אבל יש לנו איזומורפיזם). אבל ההעקה $t_i \to (-1)^i t_i$ היא אוטומורפיזם של $K(t_1, \ldots, t_n)$. היא ההופכית של עצמה לכן אוטומורפיזם של E. והוא מעתיק את מקדמים של f על המקדמים של g.

□

משפט. יהי K שדה סופי, $|K| = q$, $\tilde{K}$ הסגור האלגברי.

1. ההעתקה $\varphi_q : \tilde{K} \to \tilde{K}$ הנתונה ע"י $x \mapsto x^q$ היא אוטומורפיזם-K של $\tilde{K}$. נקרא אוטומורפיזם *Frobenius*.
2. תהי K_n ההרחבה היחידה מפעלה n של K בתוך $\tilde{K}$. אז K_n/K גלואה, $\text{Gal}(K_n/K) = \langle \varphi_q|_{K_n} \rangle$ מעגלית מסדר n.

הוכחה.

1. q חזקה של $0 < p = \text{char}\, K$ לכן $(x + y)^q = x^q + y^q$, כמובן $(xy)^q = x^q y^q$ לכן φ_q הומומורפיזם. $K = K_1 \{x \in \tilde{K} | x^q = x\}$, $\varphi_q|_K = 1$ לכן ממשפט φ_q אוטומורפיזם.
2. אכן גלואה מסדר n (כבר הוכחנו אבל לא במילים האלה). די להוכיח ש- $m := \text{ord}(\varphi_q|_{K_n}) = n$. אכן, $(\varphi_q|_{K_n})^m = 1$ לכן, לכל $x \in K_n$, $\varphi_q^m(x) = x$ כלומר $xq^m = x$. כלומר $x \in K_m$. כלומר $K_n \subseteq K_m$ לכן $n \leq m$. מצד שני, $m || \text{Gal}(K_n/K)| = n$ לכן $m \leq n$ ולכן $m = n$.

□

הערה. $\varphi_{p^k} = \varphi_p^k$. ואכן $x^{p^k} = (((x^p)^p)^p \ldots)^p$.

חבורת גלואה של פולינומים

הגדרה. יהי K שדה, $f \in K[x]$ מתוקן, פריד (אין לו שורשים מרובים בסגור האלגברי) יהי L שדה הפיצול של f בתוך $\tilde{K}$ אז $f = (x-\alpha_1)\dots(x-\alpha_n)$, $\alpha_1,\dots,\alpha_n \in L$, $L = K(\alpha_1,\dots,\alpha_n)$. נסמן $A = \{\alpha_1,\dots,\alpha_n\}$ אז L/K הרחבת גלואה סופית. אם $\alpha \in A$ שורש של f $\sigma \in \mathrm{Gal}(L/K)$ אז $\sigma(\alpha) \in A$. לכן $\sigma|_A \in S(A)$ אוסף כל התמורות של A. כמוכן $\sigma \mapsto \sigma|_A$ היא הומומורפיזם של חבורות $\mathrm{Gal}(L/K) \to S(A)$. הוא חח"ע: אם $\sigma|_A = 1$ אז $\sigma(\alpha_i) = \alpha_i$ לכל i ולכן $\sigma = id$ כי השדה נוצר ע"י α_i ולכן הגרעין הוא טריוויאלי. התמונה היא תת חבורה של $S(A)$. נסמן אותה ב- $\mathrm{Gal}(f,K)$ והיא נקראת חבורת הגלואה של f מעל K. מתקיים: $\mathrm{Gal}(f,K) \cong \mathrm{Gal}(L/K)$. בדרך כלל נזהה את A עם $\{1,\dots,n\}$ ואז נזהה את $\mathrm{Gal}(f,k)$ עם תת חבורה של S_n (אבל הזיהוי הזה תלוי בזיהוי $A \leftrightarrow \{1,\dots,n\}$).

מסקנה. $|\mathrm{Gal}(f,K)|$ מחלק את $n!$ כאשר n מעלת הפולינום (כי $|S(A)| = n!$).

למה. f אי פריק $\Leftrightarrow$ $\mathrm{Gal}(f,K)$ טרנזיטיבית.

הגדרה. חבורת תמורות G על קבוצה A נקראת טרנזיטיבית אם לכל $\alpha,\alpha' \in A$ יש $\tau \in G$ כך ש- $\tau(\alpha) = \alpha'$.

הוכחה. אם f אי פריק, ממשפט לכל $\alpha,\alpha' \in A$ יש הומומורפיזם- K יחיד $\sigma : K(\alpha) \to_K \tilde{K}$ המעביר α ל- α'. σ ניתן להרחבה להומומורפיזם $\tilde{K} \to \tilde{K}$ וצמצומו ל- L (שדה הפיצול) הוא $G \in \mathrm{Gal}(L/K)$ כל ש- $\sigma(\alpha) = \alpha'$ לכן $\tau = \sigma|_A$ מקיים $\tau(\alpha) = \alpha$. אם f פריק נאמר $f = f_1 f_2$ אז בה"כ:

$$f_1 = (x-\alpha_1)\dots(x-\alpha_m) \qquad f_2 = (x-\alpha_{m+1})\dots(x-\alpha_n)$$

$1 \le m \le n-1$. אם $\sigma \in \mathrm{Gal}(L/K)$ אז $\sigma(\alpha_1)$ שורש של f_1 לכן לא יכול להיות $\sigma(\alpha_1) \neq \alpha_n$. לכן, $(\sigma|_A)(\alpha) \neq \alpha_n$. לכן, $\mathrm{Gal}(f,K) = \{\sigma|_A|\sigma\}$ אינה טרנזיטיבית. □

דוגמא. יהי K_0 שדה ויהי $K = K_0(f_1,\dots,f_n)$ כאשר $t_1,\dots,t_n$ משתנים מעל K_0 אז $f = x^n + t_1 x^{n-1} + \dots + t_n \in K[x]$ הפולינום הכללי ממעלה n מקיים $\mathrm{Gal}(f,K) \cong S_n$.

משפט. משפט אי הפריקות של הילברט
ניקח פולינום $g(t_1,\dots,t_n,x) \in \mathbb{Q}[t_1,\dots,t_n][x]$. אז יש $a_1,\dots,a_n \in \mathbb{Q}$ כך ש- $g(a_1,\dots,a_n,x) \in \mathbb{Q}[x]$ מקיים: $\mathrm{Gal}(g(a_1,\dots,a_n,x),\mathbb{Q}) \cong \mathrm{Gal}(g(t_1,\dots,t_n),\mathbb{Q}(t_1,\dots,t_n))$.

ללא הוכחה.

משפט. יש $L/\mathbb{Q}$ גלואה כך ש- $\mathrm{Gal}(L/\mathbb{Q}) = S_n$.

הילברט גם הוכיח שיש $L/\mathbb{Q}$ גלואה כך ש- $\mathrm{Gal}(L/\mathbb{Q}) = A_n$.
בעיית גלואה ההפוכה: תהי G חבורה סופית. האם יש $L/\mathbb{Q}$ גלואה כך ש- $\mathrm{Gal}(L/\mathbb{Q}) \cong G$?
זאת שאלה פתוחה.

משפט. שפרביץ' 35
התשובה היא כן אם G פתירה. כלומר $G = G_0 \lhd G_1 \lhd \dots \lhd$ כאשר G_i/G_{i+1} אבלית.

גם ללא הוכחה.