20/4/09

אלגברה ב' - 2 שיעור 10

הגדרנו: יהי $f\in F[x]$ פולינום מדרגה $n>0$. הרחבה $F\subset L$ הינה שדה פיצול עבור f מעל F אם:

1) $f(x)=c(x-\alpha_1)\cdots(x-\alpha_n)$ $\quad \alpha_i\in L$

2) $L=F(\alpha_1,\dots,\alpha_n)$

נרצה להוכיח כי שדה פיצול הינו יחיד עד כדי איזומורפיזם. ננסח בצורה יותר כללית. נניח כי $\varphi:F_1\to F_2$ הינו איזומורפיזם של שדות ויהי $f_1\in F_1[x]$ פולינום שדרגתו $n>0$. אם נפעיל את φ על מקדמי f_1 נקבל פולינום $\varphi(f_1)=f_2\in F_2[x]$ שדרגתו היא n. עבור $i=1,2$ יהיו L_i שדות פיצול של f_i.

$$\begin{array}{ccc} L_1 & & L_2 \\ \cup & & \cup \\ F_1 & \xrightarrow{\varphi} & F_2 \end{array}$$

משפט 5.1.6: בסימונים הנ"ל, בהינתן $f_1\in F_1[x]$ ואיזומורפיזם $\varphi:F_1\to F_2$, קיים איזומורפיזם יחיד $\bar\varphi:L_1\to L_2$ כך ש: $\varphi=\bar\varphi|_{F_1}$.

הוכחה: באינדוקציה על $n=\deg f_1=\deg f_2$. אם $n=1$ אז ממשפט 5.1.5 (שאמר כי $[L:F]\le n!$) נובע $L_i=F_i$ עבור $i=1,2$ ואז $\bar\varphi=\varphi$. מההגדרה, L_1 מכיל את כל שורשי f_1 שנסמנם $\alpha_1,\dots,\alpha_n$. נסמן $g_1=\frac{f_1}{x-\alpha_1}$ ואז ניתן לבנות את סדרת ההרחבות $F_1\subset F_1(\alpha_1)\subset L_1$. L_1 הינו שדה הפיצול של g_1 מעל $F_1(\alpha_1)$.

צעד 1: נסמן $h_1\in F_1[x]$ את הפולינום המינימלי של α_1 מעל F_1. כיוון ש- $h_1(\alpha_1)=f(\alpha_1)=0$ נובע כי $h_1|f_1$ אז h_1 הינו רכיב אי-פריק של f_1 מעל F_1. לכן:

$$F_1(\alpha_1)=F_1[\alpha_1]\cong \frac{F_1[x]}{\langle h_1\rangle}$$

איזומורפיזם זה שולח את α_1 למקום $x+\langle h_1\rangle$.

צעד 2: נתאים ל-α_1 שורש של f_2. האיזומורפיזם φ משרה איזומורפיזם $\tilde\varphi:F_1[x]\to F_2[x]$, כך ש: $\tilde\varphi(f_1)=f_2$. איזומורפיזם זה מעתיק פולינום אי-פריק לאי-פריק ולכן יעתיק את h_1 לרכיב אי-פריק h_2 של f_2. לכן h_2 מתפצל ב-L_2 כי f_2 מתפצל ב-L_2. יהיו $L_2\ni\beta_1,\dots,\beta_n$ שורשי f_2, ונסמנם כך ש-β_1 הינו שורש של

h_2. h_2 הינו הפולינום המינימלי של β_1 מעל F_2.

צעד 3: השורש β_1 נותן הרחבה של שדות $F_2 \subset F_2(\beta_1) \subset L_2$. כמו כן L_2 הינו שדה פיצול עבור $g_2=\frac{f_2}{x-\beta_1}$ מעל $F_2(\beta_1)$. כמו בצעד 1 נקבל את האיזומורפיזם

$$F_2(\beta_1)=F_2[\beta_1]\cong F_2[x]/\langle h_2\rangle$$

איזומורפיזם זה שולח את β_1 לקוסט $x+\langle h_2\rangle$.

צעד 4: כיוון שהאיזומורפיזם $\tilde{\varphi}: F_1[x]\to F_2[x]$ מעתיק את h_1 ל-h_2, הוא מעתיק את האידיאל $\langle h_1\rangle$ לאידיאל $\langle h_2\rangle$. לכן

$$F_1[x]/\langle h_1\rangle \cong F_2[x]/\langle h_2\rangle$$

זהו איזומורפיזם של חוגים המעתיק את $x+\langle h_1\rangle$ ל-$x+\langle h_2\rangle$. בצמצום איזומורפיזם זה ל-F_1 מתלכד עם φ. אם נחבר צעד זה עם צעדים 1 ו-3 נקבל שקיים איזומורפיזם

$$F_1(\alpha_1)\cong F_1[x]/\langle h_1\rangle \cong F_2[x]/\langle h_2\rangle \cong F_2(\beta_1)$$

נסמן איזומורפיזם זה ב-φ_1. אז $\varphi_1(\alpha_1)=\beta_1$ וגם $\varphi_1|_{F_1}=\varphi$.

~~צעד 5: כיוון ש-φ_1 מעתיק את $F_1(\alpha_1)$ ל-$F_2(\beta_1)$,~~

צעד 5: מכיוון ש-$\varphi_1: F_1(\alpha_1)\to F_2(\beta_1)$ מעתיק את α_1 ל-β_2 ואת f_1 ל-f_2 אז הוא מעתיק את $g_1=\frac{f_1}{x-\alpha_1}$ ל-$g_2=\frac{f_2}{x-\beta_1}$.

$$\begin{array}{ccc}
L_1 & & L_2 \\
\cup & & \cup \\
F_1(\alpha_1) & \xrightarrow{\varphi_1} & F_2(\beta_1) \\
\cup & & \cup \\
F_1 & \xrightarrow{\varphi} & F_2
\end{array}$$

באמצעות הצעדים שהוכחנו נראה באינדוקציה כי קיים איזומורפיזם בין L_1 לבין L_2. כיוון שדרגת g_1 היא $n-1$ נפעיל את האינדוקציה על $g_1\in F_1(\alpha_1)[x]$ ועל $\varphi_1: F_1(\alpha_1)\to F_2(\beta_1)$. אז קיים איזומורפיזם $\bar{\varphi}: L_1\to L_2$ כך שצמצומו ל-$F_1(\alpha_1)$ הוא φ_1. כיוון ש-$\varphi=\varphi_1|_{F_1}$ נובע מכך כי $\varphi=\bar{\varphi}|_{F_1}$. ∎

אם נפעיל משפט זה על $1|_F : F \to F$ נקבל:

<u>מסקנה</u> <u>5.1.7</u>: אם L_1 ו- L_2 הם שדות פיצול של פולינום $f\in F[x]$, אז קיים איזומורפיזם $L_1 \simeq L_2$ כך שצמצומו ל- F הינו 1_F.

<u>טענה</u> <u>5.1.8</u>: יהי L שדה הפיצול של פולינום כלשהו ב- $F[x]$. יהי h פולינום אי-פריק מעל F ונניח כי יש לו שני שורשים $\alpha,\beta\in L$. אז קיים איזומורפיזם $\sigma: L\to L$ כך ש- $\sigma(\alpha)=\beta$ וגם $\sigma|_F = 1_F$.

<u>הוכחה</u>: h הינו הפולינום המינימלי של α ו- β מעל F. לכן קיימים האיזומורפיזמים

$$F(\alpha)=F[\alpha]\simeq F[x]/\langle h\rangle \simeq F[\beta]=F(\beta)$$

איזומורפיזמים אלו הם הזהות על F, ומעתיקים את α ל- $x+\langle h\rangle$ ואת $x+\langle h\rangle$ ל- β. לכן הרכבתם נותנת $\varphi: F(\alpha)\to F(\beta)$ כך ש- $\varphi(\alpha)=\beta$ וגם $\varphi|_F=1_F$. נתון כי L הינו שדה הפיצול של פולינום $f\in F[x]$, כיוון ש- $f\in F(\alpha)[x]$ וגם $f\in F(\beta)[x]$ אז L הינו שדה הפיצול של f מעל $F(\alpha)$ וגם מעל $F(\beta)$. נתונה לנו הדיאגרמה הבאה:

$$\begin{array}{ccc} L & & L \\ \cup & & \cup \\ F(\alpha) & \xrightarrow{\varphi} & F(\beta) \\ \cup & & \cup \\ F & \xrightarrow{1_F} & F \end{array}$$

כיוון ש- $1_F = \varphi|_F$, אז φ מעתיקה את f לעצמו. ממשפט 5.1.6 קיים איזומורפיזם $\bar{\varphi}: L\to L$ כך ש: $\bar{\varphi}|_{F(\alpha)}=\varphi$.
$\sigma=\bar{\varphi}$ הינו האיזומורפיזם המבוקש. ☒

<u>דוגמה</u> <u>5.1.9</u>: $L=\mathbb{Q}(\sqrt{2})$ הוא שדה הפיצול של הפולינום x^2-2 מעל $\mathbb{Q}$, פולינום זה הינו אי-פריק ושורשיו הם $\pm\sqrt{2}$. מטענה 5.1.8 קיים $\sigma: L\to L$ איזומורפיזם כך ש: $\varphi(\sqrt{2})=-\sqrt{2}$ וגם $\sigma|_{\mathbb{Q}}=1_{\mathbb{Q}}$. (במפורש

$\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2} : a,b\in\mathbb{Q}\}$

$\sigma(a+b\sqrt{2})=a-b\sqrt{2}$

הוא האיזומורפיזם המבוקש.

פונקציות סימטריות (סקירה מהירה של הנושא)

פולינום $f(x_1,\dots,x_n)$ נקרא סימטרי, אם לכל תמורה $\sigma\in S_n$ מתקיים:

$$f(x_{\sigma(1)},\dots x_{\sigma(n)}) = f(x_1,\dots,x_n)$$

לדוגמה, אם $n=3$ אז $x_1^r+x_2^r+x_3^r$ הינו סימטרי.

לכל $1\le k\le n$, הפולינום

$$s_k(x_1,\dots,x_n) = \sum_{\substack{i_1,\dots,i_k \\ i_1<\dots<i_k}} x_{i_1}x_{i_2}\cdot\dots\cdot x_{i_k}$$

נקרא הפולינום הסימטרי האלמנטרי ה-k-י.

אם $n=3$ הפולינומים הסימטרים האלמנטריים הם:

$$s_1 = x_1+x_2+x_3 \qquad s_2 = x_1x_2+x_1x_3+x_2x_3 \qquad s_3 = x_1x_2x_3$$

המשפט היסודי של הפונקציות הסימטריות קובע כי כל פונקציה (פולינומית) סימטרית הינה פולינום במשתנים $s_1,\dots,s_n$.

לדוגמה:

$$x_1^2+x_2^2+x_3^2 = (x_1+x_2+x_3)^2 - 2(x_1x_2+x_1x_3+x_2x_3) = s_1^2 - 2s_2$$

יהי $f(x)\in F[x]$ פולינום כלשהו ונניח כי שורשיו הם $a_1,\dots,a_n$ ונרשום:

$$f(x) = c(x-a_1)\cdot\dots\cdot(x-a_n) = c\left[x^n-(a_1+\dots+a_n)x^{n-1}+(a_1a_2+a_1a_3+\dots)x^{n-2}+\dots+\right.$$
$$\left.+(-1)^n a_1a_2\cdot\dots\cdot a_n\right] = c\left[x^n - s_1(a_1,\dots,a_n)x^{n-1}+s_2(a_1,\dots,a_n)x^{n-2}+\dots+\right.$$
$$\left.+(-1)^n s_n(a_1,\dots,a_n)\right]$$

כלומר מקדמי f הינם הפולינומים הסימטרים האלמנטרים מחושבים בנקודה $(a_1,\dots,a_n)$. לכן אם $f\in F[x]$ ואם $a_1,\dots,a_n\in L$ הם כל שורשי $f(x)$ אז לכל k, $s_k(a_1,\dots,a_n)\in F$.

לכן מהמשפט היסודי של הפולינומים הסימטרים נובע כי $p(a_1,\dots,a_n)\in F$ לכל פולינום סימטרי p מעל F.

5.2 הרחבות נורמליות

לא כל שדה הינו שדה פיצול של פולינום כלשהו.

<u>טענה 5.2.1</u>: יהי L שדה הפיצול של $f\in F[x]$. יהי $g\in F[x]$ אי-פריק. אם ל-g יש שורש ב-L אז <u>כל</u> שורשי g נמצאים ב-L.

<u>דוגמה 5.2.2</u>: $\mathbb{Q}(\sqrt[3]{2})$ אינו שדה פיצול עבור פולינום כלשהו. כי אם ניקח את הפולינום x^3-2, זהו פולינום אי-פריק מעל $\mathbb{Q}$. $\sqrt[3]{2}$ הוא שורש, אך שני האחרים אינם ממשיים ולכן אינם ב-$\mathbb{Q}(\sqrt[3]{2})$