23/3/09

אלגברה ב' 2 - שיעור 7

למה 4.1.13: נניח כי $F\subset L$ הינה הרחבה של שדות. יהי $\alpha\in L$ אלגברי מעל F ויהי $p(x)\in F[x]$ הפולינום המינימלי של α. אז קיים איזומורפיזם יחיד של חוגים $F[\alpha]\cong F[x]/\langle p\rangle$ שהוא קבוע על F, ושולח את α לקוסט $x+\langle p\rangle$.

הערה: כיוון ש-p אי-פריק אז $\langle p\rangle$ הינו מקסימלי, לכן $F[x]/\langle p\rangle$ הינו שדה ולכן $F[\alpha]$ הוא שדה.

טענה 4.1.14: נניח כי $F\subset L$ הרחבה של שדות. יהי $\alpha\in L$. אז α אלגברי מעל F אם ורק אם $F[\alpha]=F(\alpha)$.

הוכחה: אם α אלגברי מעל F אז מלמה 4.1.13 נקבל כי $F[\alpha]$ הינו שדה המכיל את F ואת α, כיוון ש-$F(\alpha)$ הינו השדה הקטן ביותר המכיל את F ו-α נובע מכך ש: $F(\alpha)\subseteq F[\alpha]$.
ההכלה ההפוכה תמיד מתקיימת, ולכן יש שוויון.
בכיוון ההפוך: נניח כי $F[\alpha]=F(\alpha)$. אם $\alpha=0$ אז α אלגברי.
לכן ניתן להניח כי $\alpha\neq 0$. אזי $\frac{1}{\alpha}\in F(\alpha)=F[\alpha]$. לכן קיימים $a_i\in F$ כך שמתקיים:
$$\frac{1}{\alpha}=a_0+a_1\alpha+\dots+a_m\alpha^m$$
ולכן:
$$0=-1+a_0\alpha+a_1\alpha^2+\dots+a_m\alpha^{m+1}$$
ומכאן ש-α אלגברי מעל F. ■

טענה 4.1.15: נניח כי $F\subset L$ הרחבה של שדות, ונניח כי $\alpha_1,\dots,\alpha_n\in L$ אלגבריים מעל F. אז:
$$F[\alpha_1,\dots,\alpha_n]=F(\alpha_1,\dots,\alpha_n)$$
הוכחה: מההוכחה של טענה 4.1.14 מספיק להוכיח כי $F[\alpha_1,\dots,\alpha_n]$ הינו שדה. את זה ניתן לעשות באינדוקציה על n: עבור $n=1$, זה נובע מטענה 4.1.14. נניח כי $n>1$, ונניח כי $F[\alpha_1,\dots,\alpha_{n-1}]$ הינו שדה. כיוון ש-α_n אלגברי מעל F, אז מההכלה $F\subset F[\alpha_1,\dots,\alpha_{n-1}]$ נובע כי α_n אלגברי מעל $F[\alpha_1,\dots,\alpha_{n-1}]$.
מטענה 4.1.14 נקבל כי $K=F[\alpha_1,\dots,\alpha_{n-1}][\alpha_n]$ הינו שדה. מהשוויון
$$F[\alpha_1,\dots,\alpha_{n-1}][\alpha_n]=F[\alpha_1,\dots,\alpha_n]$$
נובע כי $F[\alpha_1,\dots,\alpha_n]$ הינו שדה. ■

דוגמה: מטענה 4.1.15 נקבל כי $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}[\sqrt{2},\sqrt{3}]$. לכן כל איבר ב- $\mathbb{Q}(\sqrt{2},\sqrt{3})$ הינו פולינום במשתנים $\sqrt{2},\sqrt{3}$. כיוון ש: $(\sqrt{2})^{2n}=2^n\in\mathbb{Q}$, $(\sqrt{2})^{2n+1}=2^n\sqrt{2}$, וכנ"ל לגבי $\sqrt{3}$. לכן:
$$\mathbb{Q}(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d\in\mathbb{Q}\}$$
($\sqrt{6}=\sqrt{2}\cdot\sqrt{3}$). בהמשך נראה כי הצגה זו הינה יחידה.

הגדרה: יהיו $\alpha_1,\dots,\alpha_n$ אלגבריים מעל $\mathbb{Q}$. לשדה $\mathbb{Q}(\alpha_1,\dots,\alpha_n)$ קוראים **שדה מספרים**.

דרגה של הרחבה

אם $F\subset L$ הרחבה של שדות, אזי L הינו מרחב וקטורי מעל השדה F.

הגדרה 4.3.1: תהי $F\subset L$ הרחבה של שדות. נאמר שההרחבה היא **סופית** אם L הוא מרחב וקטורי **ממימד סופי** מעל F.
דרגת ההרחבה, שתסומן $[L:F]$ מוגדרת להיות המימד של L כמרחב וקטורי מעל F. אם ההרחבה סופית אז $[L:F]<\infty$. אחרת נאמר שההרחבה **אינסופית**, ונגדיר $[L:F]=\infty$.

דוגמה: $\mathbb{R}\subset\mathbb{C}$ הינה הרחבה סופית, ומתקיים $[\mathbb{C}:\mathbb{R}]=2$ (כל איבר ב-$\mathbb{C}$ ניתן לרשום בצורה $a+bi$, $a,b\in\mathbb{R}$)

למה 4.3.3: תהי $F\subset L$ הרחבה של שדות. אז $[L:F]=1$ אם ורק אם $L=F$.

טענה 4.3.4: תהי $F\subset L$ הרחבה של שדות, ונניח כי $\alpha\in L$. אזי:
1) α אלגברי מעל F אם ורק אם $[F(\alpha):F]<\infty$.
2) יהי α אלגברי מעל F. יהי n דרגת הפולינום המינימלי של α מעל F. אז $1,\alpha,\alpha^2,\dots,\alpha^{n-1}$ הינו בסיס עבור $F(\alpha)$ מעל F. בפרט $[F(\alpha):F]=n$.

הוכחה: נניח כי α אלגברי מעל F עם פולינום מינימלי $p(x)\in F[x]$. נניח כי $n=\deg p(x)$. נראה כי $1,\alpha,\dots,\alpha^{n-1}$ הינו בסיס ל-$F[\alpha]$ מעל F.
כיוון ש-$F(\alpha)=F[\alpha]$, אז כל איבר ב-$F(\alpha)$ הינו מהצורה $g(\alpha)$ כאשר $g(x)\in F[x]$. נחלק ונקבל:
$$g(x)=q(x)p(x)+(a_0+a_1x+\dots+a_{n-1}x^{n-1})$$
נציב $x=\alpha$ ונקבל
$$g(\alpha)=\sum_{i=0}^{n-1}a_i\alpha^i$$
לכן $\{1,\alpha,\dots,\alpha^{n-1}\}$ קבוצה פורשת.
כדי להראות שקבוצה זו בלתי תלויה, נרשום $0=\sum_{i=0}^{n-1}a_i\alpha^i$, ($a_i\in F$).
לכן α הוא שורש של $\sum_{i=0}^{n-1}a_ix^i$ ומכיוון ש-$n=\deg p$ זהו בהכרח פולינום האפס, ולכן $a_i=0$ לכל i. כלומר $\{1,\alpha,\dots,\alpha^{n-1}\}$ בסיס ל-$F(\alpha)$ מעל F ולכן $[F(\alpha):F]=n$.
כדי לסיים את ההוכחה נשאר להוכיח כי אם $[F(\alpha):F]<\infty$ אז α אלגברי. נניח כי $[F(\alpha):F]=n$. אז כל קבוצה בת $n+1$ איברים היא תלויה. לכן, קיימים $a_i\in F$, לא כולם אפס, כך ש-$\sum_{i=0}^{n}a_i\alpha^i=0$. לכן α הינו שורש של $\sum_{i=0}^{n}a_ix^i$ ולכן אלגברי מעל F. ∎

דוגמאות: 1) $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})$. הפולינום המינימלי של $\sqrt{2}$ הינו x^2-2. לכן

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

2) עבור $\sqrt{2}+\sqrt{3}$, הפולינום המינימלי מעל $\mathbb{Q}$ הינו x^4-10x^2+1.
לכן כל איבר $\beta\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$ ניתן לרשום בצורה יחידה:

$$\beta=a+b(\sqrt{2}+\sqrt{3})+c(\sqrt{2}+\sqrt{3})^2+d(\sqrt{2}+\sqrt{3})^3 \qquad a,b,c,d\in\mathbb{Q}$$

3) כיוון ש- $x\in F(x)$ אינו אלגברי מעל F, אז $[F(x):F]=\infty$.

<u>משפט 4.3.8 (משפט המגדל)</u>: נתונה הרחבה של שדות $F\subset K\subset L$.

1) אם $[K:F]=\infty$ או $[L:K]=\infty$ אז $[L:F]=\infty$.

2) אם $[K:F]<\infty$ וגם $[L:K]<\infty$ אז מתקיים: $[L:F]=[L:K][K:F]$.

<u>הוכחה</u>: 1) נוכיח כי אם $[L:F]<\infty$ אז $[K:F]<\infty$ וגם $[L:K]<\infty$.
יהי $\gamma_1,\dots,\gamma_N$ בסיס ל-L מעל F. מכיוון ש- $K\subset L$ הינו תת-מרחב מעל F אז מימדו סופי מעל F ולכן $[K:F]<\infty$.
יהי $\alpha\in L$. אז $\alpha\in\sum_{i=1}^{N}a_i\gamma_i$ עבור $a_i\in F$. כיוון ש- $F\subset K$ אז כל $\alpha\in L$ הינו צירוף לינארי של $\{\gamma_1,\dots,\gamma_N\}$ עם מקדמים ב-K.
לכן $\{\gamma_1,\dots,\gamma_N\}$ פורשת את L כמרחב וקטורי מעל K, ולכן יש לו בסיס. מכאן $[L:K]<\infty$.

2) נניח כי $m=[K:F]$ ו- $n=[L:K]$. יהי $\{\alpha_1,\dots,\alpha_m\}$ בסיס ל-K מעל F ויהי $\{\beta_1,\dots,\beta_n\}$ בסיס ל-L מעל K. נוכיח כי $\left\{\alpha_i\beta_j \,:\, \begin{smallmatrix}1\le i\le m\\ 1\le j\le n\end{smallmatrix}\right\}$ הינו בסיס של L מעל F.
כדי להראות שזו קבוצה פורשת, יהי $\gamma\in L$. נרשום $\gamma=\sum_{j=1}^{n}b_j\beta_j$ כאשר $b_j\in K$. לכל $1\le j\le n$, $b_j=\sum_{i=1}^{m}a_{ij}\alpha_i$ כאשר $a_{ij}\in F$.
לכן:

$$\gamma=\sum_{j=1}^{n}\left(\sum_{i=1}^{m}a_{ij}\alpha_i\right)\beta_j=\sum_{i,j}a_{ij}\alpha_i\beta_j$$

כדי להוכיח אי-תלות, נניח כי

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m}a_{ij}\alpha_i\right)\beta_j=0 \qquad (a_{ij}\in F)$$

כיוון ש- $\{\beta_1,\dots,\beta_n\}$ בסיס אז לכל j מתקיים $\sum_{i=1}^{m}a_{ij}\alpha_i=0$
כיוון ש- $\{\alpha_1,\dots,\alpha_m\}$ בסיס, $a_{ij}=0$ לכל i,j. ■

<u>דוגמה</u>: מהי הדרגה של ההרחבה $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$? נשתמש בהכלה:

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$$

לפי משפט המגדל:

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$$

x^2-2 הינו הפולינום המינימלי של $\sqrt{2}$ מעל $\mathbb{Q}$, ולכן $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. מתרגיל

כיוון ש- x^2-3 הוא הפולינום המינימלי של $\sqrt{3}$ מעל $\mathbb{Q}(\sqrt{2})$. לכן:
$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$

ולכן $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$.

מהוכחת המשפט נובע כי $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ הינו בסיס ל- $\mathbb{Q}(\sqrt{2},\sqrt{3})$ מעל $\mathbb{Q}$.

מתקיים $\mathbb{Q}(\sqrt{2},\sqrt{3}) \supset \mathbb{Q}(\sqrt{2}+\sqrt{3}) \supset \mathbb{Q}$. ראינו כי הפולינום המינימלי של $\sqrt{2}+\sqrt{3}$ מעל $\mathbb{Q}$ הוא ממעלה 4. לכן $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4 \Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$