תרגיל 6 - מבנים ב

בן ריפ
322657529

1 א) בסיס אינדוקציה $n=1$:

$\Gamma_n=\{1\}$ $\quad \Phi_n(x)=x-1 \in \mathbb{Q}[x]$ (1)

נניח את נכונות הטענה לכל $1\le k<n$ ונראה נכונות עבור n:

$$x^n-1=\prod_{d|n}\Phi_d(x)=\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x)\cdot\Phi_n(x) \quad (*)$$

לפי הנחת האינדוקציה כל $\Phi_d(x)\in\mathbb{Q}[x]$ ב- $(*)$ כי $1\le d<n$ ולכן $(*)\in\mathbb{Q}[x]$

ולכן מכיוון שתוצר פולינום רציונלי (x^n-1) בפולינום רציונלי ($\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x)$) נותן פולינום רציונלי (כנאמר לעיל) נקבל ש:

$$\Phi_n(x)\in\mathbb{Q}[x]$$

1 ב) נראה באינדוקציה כללית כי $\Phi_n(x)$ מתוקן ולכל מהמסקנה מהתרגיל מכיוון שמתקיים $x^n-1=\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x)\cdot\Phi_n(x)$ וכולם פולינומים ב- $\mathbb{Z}[x]$

נקבל ישירות כי כולם פולינומים ב- $\mathbb{Z}[x]$.

$n=1$: $\Phi_n(x)=x-1$ ✓

נניח כי $\Phi_k(x)$ מתוקן לכל $1\le k<n$

ונקבל $x^n-1=\prod_{\substack{d|n\\ d\neq n}}\Phi_d(x)\cdot\Phi_n(x)$

מכיוון שכאשר $d|n$, $d\neq n$ מתקבל $1\le d<n$

~~ומכיוון ש- $\Phi_d(x)$ הוא מקדם עיקרי~~

כי- $\Phi_d(x)$ מתוקן לכל d במכפלה שלנו

ולכן $\prod_{d|n, d\neq n} \Phi_d(x)$ מתוקן (כי כפל של מתוקנים

שם מתוקן). $\prod_{d|n, d\neq n} \Phi_d(x) \in \mathbb{Q}[x]$ מונוס

מכיוון ש- $\mathbb{Z}[x]$ סגור לכפל ולפי טענה ① -

~~ולפי~~ ולכן קיבלנו משוואה:

$$p = q \cdot \Phi_n(x)$$

כאשר q, p מתוקנים ולכן גם $\Phi_n(x)$

מתוקן וס"מ נ.

(ב) ו יתקיים $F(\alpha) \cong \mathbb{F}[x]/(m_\alpha^{\mathbb{F}}) = \mathbb{F}[x]/(m_\beta^{\mathbb{F}}) \cong F(\beta)$

$$\Downarrow$$

$F(\alpha) \cong F(\beta)$ ולכן Φ קיים.

איבר כללי ב- $F(\alpha)$ הינו מהצורה

$\sum_{i=0}^{n} a_i \alpha^i$ כאשר $n = \deg m_\alpha^{\mathbb{F}} - 1$ $\quad a_i \in \mathbb{F}$

מהגדרה: a_i יחידים לכל $x \in F(\alpha)$

$$\Phi\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} \Phi(a_i)\Phi(\alpha)^i = \sum_{i=0}^{n} a_i \beta^i$$

Φ הומומורפיזם של שדות

$\Phi(\alpha) = \beta$

$\Phi|_{\mathbb{F}} = id$

מהגדרה: a_i יחידים לכל $x \in F(\beta)$

מכיוון שקיבלנו נוסחה מפורשת רק בהינתן הנחנו שהשלה Φ תמיד יקיים נוסחה כזו ולכן יחיד.

הערה: במהלך ההוכחה פסמיים הסתמכנו בטענה מלינארית 1 שאומרת שאם B בסיס ל- V מ"ו מעל $\mathbb{F}$ ומתקיים $v = \sum_{i=1}^{n} a_i v_i$ $a_i \in \mathbb{F}, v_i \in B$ אזי a_i יחידים. בנוסף הסתמכנו בטענה ממבנים 1 שאם $p \in \mathbb{F}[x]$ אי פריק

$$\cancel{\deg p(x) = \dim \mathbb{F}[x]/(p(x))}$$

הקבוצה $\{1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{\deg p - 1}\}$ מהווה בסיס ל- $\mathbb{F}[x]/(p(x))$ כמ"ו מעל $\mathbb{F}$

ולכן הייצוג של $x \in F(\alpha)$ (לא אלגברי) ביצוג $x = \sum_{i=0}^{\deg m_\alpha^{\mathbb{F}} - 1} a_i \alpha^i$ יחיד.

ב) נסמן עבור $p\in F[x]$ את $\rho(p)$ בתנאי מ"ס הנורמליים הנשלטים ~~בשדה הסגור~~ ~~אלג~~. ~~נתון~~ נתון מעל F בגודל $\rho(p)$.
הראנו ~~בהרצאה~~ בהרצאה שמתקיים:

$$(*)\quad \rho(m_\alpha)=|Aut(F(\alpha)/F)|$$

באופן דומה עבור עבור β. $(*)'$

ומכיוון ש: $F(\alpha)=F(\beta)$ מתקיים:

$$\rho(m_\alpha)=|Aut(F(\alpha)/F)|=|Aut(F(\beta)/F)|$$

~~ומכיוון שמתקיים~~ ולכן $(*)$, $(*)'$ נקבל ש:

$$\rho(m_\alpha)=\rho(m_\beta)$$

מכיוון ש: $F(\alpha)=F(\beta)$ מתקיים

$$[F(\alpha):F]=[F(\beta):F]$$
$$\Downarrow$$
$$\deg m_\alpha=\deg m_\beta$$

אבל מכיוון שגם m מתפרק לגורמים לינאריים שונים מעל E מתקיים:

$$\deg m_\beta=\deg m_\alpha=\rho(m_\alpha)=\rho(m_\beta)$$
$$\Downarrow$$
$$\deg m_\beta=\rho(m_\beta)$$
$$\Downarrow$$

m_β מתפרק לגורמים לינאריים מעל E ומקיים-

3 (ב) מכיוון ש: ρ אוטומורפיזם ומקיים

$\rho(\zeta_n)^n = 1 \Leftarrow 1 = \zeta_n^n$

נסמן $x = \rho(\zeta_n) \Leftarrow x^n - 1 = 0$

$\Downarrow$

$x = \zeta_n^k \quad 1 \le k \le n$

~~נשים לב כי מכיוון ש: ρ אוטומורפיזם~~
~~בפרט מתקיים $\zeta_n = \rho^{-1}(\zeta_n)^k$~~

~~$\Downarrow$~~

נשים לב כי $m \equiv k \pmod{n} \Leftrightarrow \zeta_n^m = \zeta_n^k$

(מתרגיל קודם) בנוסף, מכיוון ש: $\rho|_{\mathbb{Q}} = id$

נקבל שלכל $x \in \mathbb{Q}(\zeta_n)$ $\Leftarrow$ $x = \sum_{i=0}^{n_0} a_i \zeta_n^i$ $\quad n_0 = \deg_{\mathbb{Q}} \zeta_n$

$\rho(x) = \rho\left(\sum_{i=0}^{n_0} a_i \zeta_n^i\right) = \sum_{i=0}^{n} a_i \zeta_n^{k \cdot i}$

מכיוון ש- ρ שמקיים x מקיים $\rho(x) = \zeta_n$

ולכן

$\sum_{i=0}^{n_0} a_i \zeta_n^{k \cdot i} = \zeta_n$

$\Downarrow$

$\exists i \in \mathbb{N}$ ~~$\exists i \in \{0, \dots, n_0\}$~~ $\zeta_n^{k \cdot i} = \zeta_n \Rightarrow k \cdot i \equiv 1 \mod n$

$\Downarrow$

$k \cdot i + c \cdot n = 1$

עקרון הכפל לסמיכן $\Leftarrow (k, n) = 1$.

3 ב) נשים לב כי $\rho_k = \rho_1 \circ \rho_k$ כאשר הכפל בין k ל-1 הוא כפל מודולו n.

נגדיר $\psi: G \to (\mathbb{Z}/n\mathbb{Z})^\times$

$$\psi(\rho_k) = k$$

לפי הגדרה ψ הומומורפיזם

~~נניח $k \neq m \bmod n \Leftarrow k = m \in \mathbb{Z}_n^\times$~~

ψ חח"ע:

נניח $\rho_k \neq \rho_m \in G$ מכיוון ש-ρ_k, ρ_m נקבעות רק לפי מה הן פועלות ל-ζ_n ~~לפי הפעולה על ζ_n והומומורפיזם לפי שדות ואוטומורפיזמים ולכן הוא~~ כי הוא האיבר שהוספנו בהרחבה הפשוטה $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ו- ρ_m, ρ_k אוטומורפיזמים לפי הרחבה זו, הראנו בכיתה שהן שונות רק בקבע שו:

$$\rho_m(\zeta_n) \neq \rho_k(\zeta_n)$$

לפי סעיף א'

$$\Downarrow$$

$$\zeta_n^m \neq \zeta_n^k$$

$$\Downarrow$$

$$m \neq k \bmod n$$

לכן ψ חח"ע.

$$\Downarrow$$

$$G \hookrightarrow \mathbb{Z}_n^\times$$

③ ד) לפי טענה קודם $\deg \Phi_n \beta = \varphi(n)$

ומתקיים שמתקיים כי $\varphi(n) = |\mathbb{Z}_n^\times|$

מכיוון ש $\Phi_n(x)$ אי פריק ומאפס את ζ_n

(ואפילו מתוקן מ-①) נקבל $m_{\zeta_n}^{\mathbb{Q}} = \Phi_n(x)$

מהרצאה הראנו כי $[F(\beta):F] = |Aut(F(\beta)/F)|$

ויודעים כי $\deg m_\beta^F = [F(\beta):F]$ אם β אלגברי.

$$\Downarrow$$

$$\cancel{\varphi(n) = |Aut(\mathbb{Q}(\zeta_n))|}$$

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n) = |Aut(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = |G|$$

ולכן מכיוון שלפי G, $\mathbb{Z}_n^\times$ יש איזו

פונקציה ופונקציה ψ מעל קודם בסך הכל

$$G \cong \mathbb{Z}_n^\times$$

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

$\mathbb{Q}(\sqrt{3})(\sqrt{2}) =$ 4 נשים לב כי מכיוון ש:

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

$$\underbrace{Aut(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}(\sqrt{3}))}_{G_{\sqrt{2}}} \cup \underbrace{Aut(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}(\sqrt{3}))}_{G_{\sqrt{3}}} \subseteq \underbrace{Aut(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q})}_{G}$$ מתקיים (*)

ומתקיים ש: $\varphi_{\sqrt{3}}: \mathbb{Q}(\sqrt{3},\sqrt{2}) \to \mathbb{Q}(\sqrt{3},\sqrt{2})$

$\varphi_{\sqrt{3}}(a+b\sqrt{3}) = a-b\sqrt{3} \quad a,b \in \mathbb{Q}(\sqrt{2})$

$\varphi_{\sqrt{2}}: \mathbb{Q}(\sqrt{3},\sqrt{2}) \to \mathbb{Q}(\sqrt{3},\sqrt{2})$

$\varphi_{\sqrt{2}}(a+b\sqrt{2}) = a-b\sqrt{2} \quad a,b \in \mathbb{Q}(\sqrt{3})$

(סימון מטל מבלבל) $\varphi_{\sqrt{2}} \in G_{\sqrt{3}}$, $\varphi_{\sqrt{3}} \in G_{\sqrt{2}} \overset{\text{לפי } (*)}{\Longrightarrow} \varphi_{\sqrt{2}}, \varphi_{\sqrt{3}} \in G$

ומתקיים ש: $\varphi_{\sqrt{3}}, \varphi_{\sqrt{2}}, \varphi_{\sqrt{3}} \circ \varphi_{\sqrt{2}}, id$ נשלים (**)

~~$\varphi_{\sqrt{3}}(\sqrt{3}) = -\sqrt{3}$~~ $\varphi_{\sqrt{2}} \circ \varphi_{\sqrt{3}} \in G$

~~$\varphi_{\sqrt{2}}(\sqrt{3}) = \sqrt{3}$~~

~~$\varphi_{\sqrt{3}}(\sqrt{3}) = -\sqrt{3}$~~

כי הרכבה זו הפעלה ב-G והיא הפיכה (המבנים ו)

~~φ~~

(**) נבין כי $\varphi_{\sqrt{2}}(\sqrt{2}+\sqrt{3}) = -\sqrt{2}+\sqrt{3}$

$\varphi_{\sqrt{3}}(\sqrt{2}+\sqrt{3}) = \sqrt{2}-\sqrt{3}$

$\varphi_{\sqrt{2}} \circ \varphi_{\sqrt{3}}(\sqrt{2}+\sqrt{3}) = \varphi_{\sqrt{2}}(\sqrt{2}-\sqrt{3}) = -\sqrt{2}-\sqrt{3}$

$id(\sqrt{2}+\sqrt{3}) = \sqrt{2}+\sqrt{3}$

לכן מכיוון שהם 4 איברים נשלים

(*) נשים לב כי מתקיים $|G| \geq 4$ קל

ולמעשה נסיק כי $G=\{id, \varphi_{\sqrt{2}}, \varphi_{\sqrt{3}}, \varphi_{\sqrt{2}}\circ\varphi_{\sqrt{3}}\}$

הוכחנו בהרצאה כי $|Aut(E/F)| \le [E:F]$ כפל"ש בדרגה

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

ולמכיוון ש: x^2-3 מאפס ע"י $\sqrt{3}$ מעל $\mathbb{Q}$

וכן x^2-2 מאפס ע"י $\sqrt{2}$ מעל $\mathbb{Q}(\sqrt{3})$

לכן מינימליים $m_{\sqrt{3}}^{\mathbb{Q}} \mid x^2-3$, $m_{\sqrt{2}}^{\mathbb{Q}(\sqrt{3})} \mid x^2-2$

$\Downarrow$

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

לכן

$|G| = |Aut(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| \le [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] \le 2\cdot 2 = 4$

4) ב) מכיוון ש:

$$\cancel{\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}[x]}$$

$$m^{\mathbb{Q}}_{\sqrt[4]{2}} = x^4 - 2$$

~~לפי~~ לפי אייזנשטיין הוא אי פריק
והרור נמתאים ומאפס את $\sqrt[4]{2}$.
לכן יש התאמה חח"ע ועל בין $Aut(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$
לשורשי $m^{\mathbb{Q}}_{\sqrt[4]{2}}$ ~~ש~~ שנמצאים ב- $\mathbb{Q}(\sqrt[4]{2})$.
שורשי x^4-2 הם $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$
אבל $\pm i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$ לכן $Aut(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \{id, \varphi\}$
כאשר

$$\varphi(\sqrt[4]{2}) = -\sqrt[4]{2}$$

ולפי טענה מהרצאה φ נקבע מיחידות
הסכה וסיימנו.