מבנים אלגבריים 2 - תרגיל בית 6.

שאלה 1:

א) ראינו ש: $x^{n}-1=\prod_{d|n}\Phi_d(x)$. נראה כי $\Phi_n\in\mathbb{Q}[x]$.

נוכיח את הטענה באינדוקציה:

עבור $n=1$: מתקיים: $\Phi_1(x)=x-1$, ובבירור $\Phi_1(x)\in\mathbb{Q}[x]$.

כעת נניח עבור n ונוכיח עבור $n+1$:

מתקיים $x^{n+1}-1=\prod_{d|(n+1)}\Phi_d(x)=\Phi_{n+1}(x)\cdot\prod_{\substack{d|(n+1)\\ d<n+1}}\Phi_d(x)$.

לפי הנחת האינדוקציה $\Phi_d(x)\in\mathbb{Q}[x]$ לכל $d\in\mathbb{N}$ כך ש $d<n+1$, ולכן גם $\underbrace{\prod_{\substack{d|(n+1)\\ d<n+1}}\Phi_d(x)}_{=(*)}\in\mathbb{Q}[x]$.

$\Leftarrow$ מאחר שחלוקת פולינום רציונלי $x^{n+1}-1$ בפולינום רציונלי $(*)$, נקבל ש $\Phi_{n+1}(x)\in\mathbb{Q}[x]$.

$\Leftarrow$ $\Phi_n(x)\in\mathbb{Q}[x]$ לכל n כנדרש.

ב) נראה כי $\Phi_n(x)$ מתוקן קודם:

$n=1$: $\Phi_1(x)=x-1$ $\Leftarrow$ בבירור מתוקן.

נניח עבור n ונוכיח עבור $n+1$. נתבונן אם כן שוב:

$$x^{n+1}-1=\prod_{d|(n+1)}\Phi_d(x)=\Phi_{(n+1)}(x)\cdot\prod_{\substack{d|(n+1)\\ d<n+1}}\Phi_d(x)$$

ע״פ ההנחה $\Phi_d(x)$ מתוקן לכל $d<n+1$, וכיוון ש $x^{n+1}-1$ מתוקן גם. נניח בשלילה ש $\Phi_{(n+1)}(x)$ אינו מתוקן $\Leftarrow$ אגף ימין אינו מתוקן בסתירה לנתון שהם שווים.

$\Leftarrow$ $\Phi_n(x)$ מתוקן לכל n כנדרש, ולכן לפי המסקנות מתרגול 6, מסקנה 3, גאוס, הוא שייך ל $\mathbb{Z}[x]$ ובפרט $\Phi_n(x)\in\mathbb{Z}[x]$

שאלה פ:

א) ראשית כל נראה קיום:

$$F(\alpha) \cong \mathbb{F}/(m_\alpha^{\mathbb{F}}) = \mathbb{F}/(m_\beta^{\mathbb{F}}) \cong F(\beta)$$

ולכן קיים איזומורפיזם ϕ כך ש $\phi: \mathbb{F}(\alpha) \longrightarrow \mathbb{F}(\beta)$.

כעת נראה יחידות:

נתבונן באיבר כלשהו $\beta(x) \in \mathbb{F}(\alpha)$ אזי ידוע שהקבוצה $\{1, \alpha, \alpha^2, \dots, \alpha^{\overset{=n}{\deg(m_\alpha^{\mathbb{F}})-1}}\}$ מהווה בסיס ל $\mathbb{F}/(m_\alpha^{\mathbb{F}})$ ~~[illegible]~~ כמ"ו מעל $\mathbb{F}$. לכן, ניתן לרשום באופן יחיד:

$$\beta(x) = \sum_{i=0}^{n} a_i \cdot (\alpha)^i \qquad (\forall i : a_i \in \mathbb{F})$$

נשים לב ש

$$\phi(\beta(x)) = \phi\left(\sum_{i=0}^{n} a_i \cdot \alpha^i\right) \underset{\text{הומומורפיזם שדות}}{=} \sum_{i=0}^{n} \phi(a_i) \cdot \phi(\alpha)^i = \dots$$

$$\dots = \sum_{i=0}^{n} a_i \cdot \beta^i$$

נשים לב ש $a_i \in \mathbb{F}$ בנוסף יחידים ולכן $\phi(\beta(x))$ נקבע ביחידות גם כן, ולכן מאחר שכבר נתון יחיד כי $\beta(x)$, ϕ איזומורפיזם נקבע באופן יחיד.

ט) $\mathbb{E}=\mathbb{F}(\alpha)$ הרחבה סופית, $m_\alpha\in\mathbb{F}[x]$ מתפרק לגורמים לינאריים מעל $\mathbb{E}$. נראה שאם $\beta\in\mathbb{E}$ פרימיטיבי המקיים $\mathbb{F}(\beta)=\mathbb{E}$ מתקיים ש $m_\beta\in\mathbb{F}[x]$ גם מתפצל לחלוטין.

ראינו שמתקיים:
$$|Aut(\mathbb{F}(\alpha)/\mathbb{F})|=\varphi(m_\alpha^{\mathbb{F}})$$

ולכן:
$$|Aut(\mathbb{F}(\beta)/\mathbb{F})|=\varphi(m_\beta(\mathbb{F}))$$

$$\varphi(m_\alpha^{\mathbb{F}})=\left|Aut\left(\mathbb{F}(\alpha)/\mathbb{F}\right)\right|=\left|Aut(\mathbb{F}(\beta)/\mathbb{F})\right|=\varphi(m_\beta^{\mathbb{F}})$$

ב) $m_\alpha^{\mathbb{F}}$ מתפצל לחלוטין! ולכן $\varphi(m_\alpha(\mathbb{F}))=\deg(m_\alpha(\mathbb{F}))$ ולכן $\varphi(m_\beta|\mathbb{F})=\deg(m_\alpha|\mathbb{F})$ אך ידוע שגם $\mathbb{F}(\alpha)=\mathbb{F}(\beta)$, ולכן בפרט $[\mathbb{F}:\mathbb{F}(\alpha)]=[\mathbb{F}:\mathbb{F}(\beta)]$ ולכן מאחר ש $\deg(m_\beta|\mathbb{F})=\deg(m_\alpha|\mathbb{F})$ מתקיים ש $\deg(m_\beta|\mathbb{F})=\varphi(m_\beta|\mathbb{F})$ ולכן בסה"כ $m_\beta^{\mathbb{F}}$ הוא מתפצל לחלוטין

שאלה 4.

נחשב את $Aut\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}\right)$.

נשים לב שמצד אחד, $[\mathbb{Q}(\sqrt{3},\sqrt{2}):\mathbb{Q}] \geq \left|Aut\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}\right)\right|$

מצד שני:

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

נשים לב ש x^2-3, x^2-2 ~~...~~ מינימליים ~~ש~~ של $\sqrt{3}$ ו-$\sqrt{2}$

בהתאמה ולכן נקבל ש:

$$\left|Aut\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}\right)\right| \overset{(*)}{\leq} 4$$

כעת נראה כי בדיוק מתקיים שוויון ב $(*)$

נשים לב ש $\mathbb{Q}(\sqrt{3}),\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{3},\sqrt{2})$. לכן

$$(*) \supseteq Aut\left(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}(\sqrt{2})\right) \cup Aut\left(-/\mathbb{Q}(\sqrt{3})\right)$$

~~...~~ האיברים בכל ~~...~~ שכל אחד מן החבורות הללו, נמצאת בתוך החבורה הנ"ל, ושונים.

נסמן $\phi_1 = id$, $\phi_2(\underset{\in \mathbb{Q}(\sqrt{2})}{a}+b\sqrt{3})=a-b\sqrt{3}$, $\phi_3(\underset{\in \mathbb{Q}(\sqrt{3})}{a}+b\sqrt{2})=a-b\sqrt{2}$

נשים לב ש $\phi_1 \neq \phi_2 \neq \phi_3$, מאחר ש $\phi_1(\sqrt{3})=\sqrt{3}$ ואילו, $\phi_2(\sqrt{3})=\sqrt{3}$

וגם $\phi_1(\sqrt{2})=\sqrt{2}$ אבל $\phi_3(\sqrt{2})=-\sqrt{2}$, וכמו כן:

$$\phi_2(\sqrt{2}+\sqrt{3}) = \sqrt{2}-\sqrt{3}$$

$$\phi_3(\sqrt{3}+\sqrt{2}) = \sqrt{3}-\sqrt{2}$$

כלומר חבורת האוטומורפיזמים לפחות בגודל 3

נסמן $\phi_4=\phi_2\circ\phi_3$, אבל זה אוטומורפיזם זה שונה מכולם

$$\phi_4(\sqrt{3}+\sqrt{2}) = \phi_2(\sqrt{3}-\sqrt{2}) = -\sqrt{3}-\sqrt{2}$$

לכן גודל החבורה הינו בדיוק 4.

Scanned by CamScanner

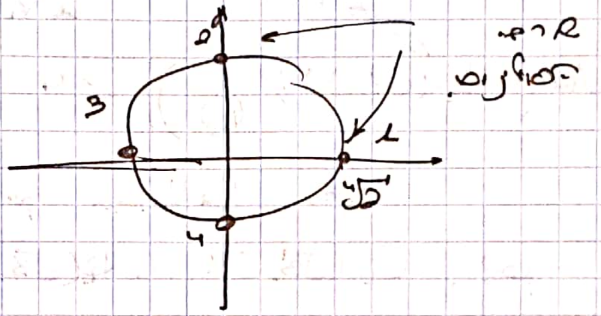
ב) כמה נספור את $Aut\left(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}\right)$ (*)

נתבונן בהרחבה $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. נשים לב ש $m_{\sqrt[4]{2}}^{\mathbb{Q}} = x^4-2$

מאחר ~~והוא~~ הוא פולינום אי פריק ~~[illegible]~~ ו- $\sqrt[4]{2}$ מאפס.

⟸ ראינו ש.ש. ~~[illegible]~~ הגדר ח"ס ולכן (*) לפי שורשי $m_{\sqrt[4]{2}}$ אשר נמצאים ב $\mathbb{Q}(\sqrt[4]{2})$.

לפי משפט מהמאמר:



נשים לב ש ③ ו- ④ לא נמצאים ב $\mathbb{Q}(\sqrt[4]{2})$ מאחר שהם מרוכבים.

⟸ $2=|Aut(*)|$. נשים לב כי נקבל בפרט את $\phi_1 = id$,

בנוסף - ϕ_2 $\sqrt[4]{2}^{2}$ ונקבל את הנדרש.